F. DELASTELLE

# CRYPTOGRAPHIE NOUVELLE

ASSURANT

## L'INVIOLABILITÉ ABSOLUE

DES

## CORRESPONDANCES CHIFFRÉES

PRIX : 3 FRANCS




PARIS
P. DUBREUIL, IMPRIMEUR-ÉDITEUR
18 BIS, RUE DES MARTYRS, 18 BIS

1893



# CRYPTOGRAPHIE NOUVELLE

---

F. DELASTELLE

# CRYPTOGRAPHIE NOUVELLE

ASSURANT

## L'INVIOLABILITÉ ABSOLUE

DES

## CORRESPONDANCES CHIFFRÉES

PRIX : 3 FRANCS




PARIS
P. DUBREUIL, IMPRIMEUR-ÉDITEUR
18 BIS, RUE DES MARTYRS, 18 BIS

1893

# INTRODUCTION

---

Chacun sait que la cryptographie a pour objet de permettre l'échange de correspondances intelligibles pour les seuls initiés et, par conséquent, à l'abri des indiscrétions possibles.

La cryptographie est un *art* et une *science*.

L'*art* rend un cryptographe exercé en état de remédier aux défectuosités du système qu'il emploie. Par exemple, la suppression ou l'addition d'une lettre, au texte d'une dépêche, suffit souvent pour rendre indéchiffrable un passage qui, sans cette modification, n'eût offert que peu ou point de difficulté à un déchiffreur habile.

Malheureusement, l'*art* ne s'acquiert que par une *longue* pratique, indépendamment des qualités, dispositions naturelles et connaissances spéciales qu'il exige de ceux qui s'y adonnent.

On ne doit pas, par suite, faire une trop grande part à l'*art*, surtout pour le service de l'armée, où, à chaque instant, un officier, dont l'esprit ne s'est peut-être jamais attaché bien sérieusement à la cryptographie, peut se trouver inopinément dans

la nécessité d'expédier et de recevoir des dépêches chiffrées.

Il est donc indispensable que les méthodes employées soient simples, claires, n'exigent, pour leur application, qu'une intelligence ordinaire et les moindres moyens matériels, n'entraînent aucune tension de l'esprit et, condition importante, puissent s'enseigner et s'acquérir en peu d'instants, tout en offrant une sécurité absolue.

Telles sont les premières qualités que l'on doit exiger d'une méthode vraiment militaire ; l'*art* ne vient donc qu'en seconde ligne.

La *science cryptographique* se divise en deux branches : l'une comprenant l'écriture et la lecture de dépêches établies suivant des conventions déterminées ; l'autre, la lecture de textes dont on ne possède pas la clé.

En considérant cette dernière dans toute sa généralité, on peut dire que c'est l'*âme* de la civilisation, l'*âme* du monde. Que font, en effet, le savant, le commerçant, le financier, l'industriel, le chasseur et même le sauvage à la recherche d'un fruit, d'une source, d'un gibier, d'un ennemi ? Ne cherchent-ils pas tous à deviner soit le passé ou le présent, soit même l'avenir, à traduire les faits observés et à en déduire les conséquences, à trouver des traces, à interpréter des indices qui les amèneront à la découverte de ce qu'ils ignorent et ont intérêt à connaître ?

Inutile de rechercher, ici, les origines de l'autre branche qui constitue la cryptographie proprement dite.

Elle est aussi ancienne que l'écriture, plus ancienne même, car avant que l'homme primitif eût

seulement songé à la possibilité de représenter ses mots ou ses idées par des signes ou des dessins quelconques, il a certainement dû, pour éviter l'un de ses semblables lancé à sa poursuite, s'efforcer d'effacer ses traces, de déguiser ses vestiges, de masquer ses empreintes et même d'en simuler d'autres, employer, en un mot, tous les moyens en son pouvoir pour détourner un ennemi acharné et le diriger sur une fauste piste.

Depuis l'invention ou plutôt la vulgarisation de l'écriture, les plus grands efforts ont été faits pour cacher aux profanes le sens des écrits de toutes sortes et même des inscriptions murales. Ici, c'est l'écriture hiératique ou hiéroglyphique, là, c'est l'écriture cunéiforme, ailleurs, c'est une langue étrangère... De nos jours encore, par suite d'on ne sait quelle vieille coutume, nous éprouvons le besoin de faire usage, dans certaines de nos inscriptions publiques, de langues étrangères, inconnues du plus grand nombre. Ce n'est certes pas pour céler le sens de ces inscriptions ; serait-ce, par hasard, dans le but de les rendre plus intelligibles ?

Au moyen âge, les savants, pour éviter que la science tombât entre des mains capables d'en abuser, ou seulement pour qu'elle ne se répandît pas trop, rendaient, de propos délibéré, leurs écrits inintelligibles au vulgaire ; quant à leurs découvertes, ils les voilaient avec un soin encore plus jaloux, craignant, à la fois, de les voir divulguées et de perdre l'honneur de les avoir faites.

Maintenant les savants parlent et écrivent encore dans des langues spéciales, à la portée seulement des initiés, mais leur but, tout différent de

celui de leurs prédécesseurs, est d'énoncer plus clairement et plus simplement leurs idées, qu'ils ne le pourraient faire avec la langue commune. Tel est le cas des mathématiciens, chimistes, médecins, géologues, etc.

Laissons de côté ces considérations et voyons en quoi consiste la cryptographie usuelle.

En faisant abstraction des livres, codes, dictionnaires chiffrés, etc., d'un emploi peu pratique dans une armée en campagne, tous les systèmes de cryptographie, même ceux qui reposent sur l'emploi d'un appareil, peuvent se ranger dans l'une ou l'autre des deux grandes classes :

*Cryptographie par substitution*, et
*Cryptographie par transposition ou anagramme.*

*
* *

*Cryptographie par substitution.* — Ce système consiste à remplacer une lettre par une autre ou par un signe quelconque, sans modifier son rang dans le document à chiffrer.

Cela revient à déguiser les lettres en leur mettant un masque, ou plutôt un faux nez, qui ne les rend méconnaissables qu'à des yeux peu exercés.

Chaque lettre a, en effet, son allure, son caractère, sa démarche, ses relations, ses goûts complètement différents de ceux des autres.

Celle-ci qui, vive et remuante, se montre partout à la fois, souvent accompagnée de ses sœurs jumelles, c'est évidemment la lettre *e*.

Celle-là, qui semble boiteuse et suit si difficilement les autres qu'on ne la rencontre guère qu'à la fin des mots, ne peut être que *z*.

En voici une, grave et fière, qui s'isole volontiers, bien qu'elle ne craigne pas de se montrer partout, même à la fin des mots, c'est certainement *a*.

*y* s'isole volontiers aussi, mais il est timide et ne s'exhibe pas avec plaisir.

Voilà maintenant un jeune page qui se plait à porter la traîne de plusieurs mots de suite ; on reconnaît *s* à cette manie.

De ces lettres qui se promènent deux à deux, l'une, au moins, est une voyelle.

Oh ! une apostrophe. La lettre suivante est forcément une voyelle, à moins cependant que ce ne soit *h*.

Mais devant l'apostrophe, il n'y a que deux lettres. Dans ce cas, nous avons, sans le moindre doute, affaire à *qu'*.

...... Décidément nos lettres ne sont pas assez déguisées ; elles sont trop faciles à reconnaître.

Les spécialistes n'ont eu garde de s'y méprendre et ils ont imaginé de les faire changer continuellement de costumes, de telle sorte que le signe par lequel *a* était, à l'instant, figuré, représente maintenant *k* ou *v*, etc. Pour cela, on emploie concurremment plusieurs alphabets, le premier servant à chiffrer les lettres qui occupent tels et tels rangs dans le texte ; le second s'appliquant aux lettres qui suivent immédiatement les premières, etc., etc.

Le travail de l'écrivain est donc, de même que celui du traducteur, notablement plus pénible et les chances d'erreur considérablement augmentées ; malgré cela, cependant, on ne parvient pas à se mettre à l'abri des indiscrétions.

**

M. Kerckhoffs a, en effet, indiqué une méthode qui permet de déterminer facilement le nombre des alphabets dont il a été fait usage dans un document de cette espèce. Il est ensuite aisé de séparer les lettres appartenant à chaque alphabet. Ce travail fait, on cherche à reconnaître quelqu'une des lettres de chaque groupe et il arrive souvent que la connaissance d'une *seule* lettre suffit pour entraîner celle de toutes les autres lettres du même alphabet.

*
* *

Dans la *Cryptographie par transposition*, les lettres ne sont plus masquées ; elles sont seulement brouillées, emmêlées l'une dans l'autre ; elles vont à la débandade sans lien, sans *ordre*, en apparence du moins. C'est un troupeau où chaque animal marche à sa guise, une joyeuse bande d'écoliers folâtrant dans la campagne.

Il semble bien difficile, lorsqu'on ne possède pas le secret de l'arrangement, de démêler cette troupe confuse. Cependant, en étudiant, comme tout à l'heure, la personnalité de chaque lettre, on verra promptement que, en prenant pour base leurs sympathies et leurs antipathies, il devient possible d'en remettre quelques unes à leurs places ; puis, celles-là servant de jalons, les autres s'alignent plus facilement et, enfin, quand un groupe est reconstitué, il ne reste plus qu'à disposer les autres d'une manière symétrique.

Tout le monde connaît les sympathies et les antipathies de la plupart des signes alphabétiques. On sait notamment que *p* et *b* refusent de mar-

cher à la suite d'une *n*, tandis que *c*, *d*, *f*, *g*, *s*, *t*, *v* repoussent *m*, l'amie de *b* et *p*.

*z* a une antipathie prononcée pour toutes les consonnes ; il boude aussi les voyelles à l'exception de *e*. Cependant à la tête d'un mot et parfois au milieu, il consent à se laisser approcher par *i* et *o*, rarement par *u* et presque jamais par *a*.

*x* boude également les consonnes, mais, bien qu'il préfère la compagnie de *ï* et *u*, il ne fuit pas les autres voyelles.

Sauf dans les deux mots : *cinq* et *coq*, *q* refuse d'avancer sans son *u* inséparable.

*h* aime à prendre le bras de *c*, sans toutefois dédaigner l'appui de *p* et de *t*.

Il serait oiseux de nous appesantir davantage sur ce sujet.

* * *

La *Cryptographie nouvelle* ne peut se ranger ni dans l'une ni dans l'autre des deux classes mentionnées ci-dessus.

Elle participe de l'une et de l'autre et tient, en outre, de la *scytale* lacédémonienne.

Dans ce système, les lettres ne se déguisent pas, elles se *transforment*. Elles ne quittent pas leurs places, elles s'évanouissent en se subdivisant en plusieurs morceaux. Chacun de ceux-ci, s'éloignant de ses frères, va se joindre à des étrangers pour reconstituer de nouvelles lettres.

En résumé, ce système présente la plus grande analogie avec ces transformations de personnages grotesques obtenus par la superposition d'images diverses et convenablement découpées. Chacun a

pu voir ces sortes d'albums, colportés sur les boulevards, où la tête d'un pompier voltige en passant successivement du corps d'une cuisinière sur celui d'un marmiton ou d'un valet de ferme...

Prenons trois de ces personnages, ou plutôt empruntons à une collection enfantine les portraits de Polichinelle, d'Arlequin et de Pierrot. Faisons trois morceaux de chacun, de manière à isoler la tête, le corps et les jambes.

A présent, formons tous les personnages possibles en associant tête, corps et jambes, sans tenir compte de leurs origines.

Il est évident que la tête de Pierrot pourra surmonter non seulement le buste de Pierrot, mais aussi celui d'Arlequin ou celui de Polichinelle.

Chacun des individus ainsi formés pourra ensuite être complété par les jambes de l'un quelconque des trois types.

La tête de Pierrot fera donc partie de *neuf corps* différents. Il en sera de même pour la tête d'Arlequin et pour celle de Polichinelle. Nous formerons ainsi *vingt-sept* personnages divers.

Or, si à l'alphabet, contenant 26 lettres, nous ajoutons le signe +, qui servira tant à la ponctuation qu'à la séparation des mots, nous aurons également *vingt-sept* signes et chacun d'eux pourra être représenté par un de nos personnages.

Attribuons un chiffre à chacun de nos individus primitifs, le même chiffre servant indifféremment pour chaque morceau. Un personnage quelconque sera alors représenté par trois chiffres, dont la position seule indiquera la partie de l'image qu'il convient de prendre.

1 représentera un *bonhomme* formé avec la tête
2 du n° 1, le buste du n° 2 et les jambes du
3 n° 3 ;

3 sera l'image composée de la tête n° 3, du buste
2 n° 2 et des jambes n° 3 ; etc.
3

Ceci convenu, pour chiffrer un texte quelconque, nous n'avons plus qu'à remplacer les lettres à transmettre par les figures qui leur correspondent, c'est-à-dire par les chiffres servant à les désigner.

Si nous nous arrêtions là, notre système offrirait peu d'avantage sur les anciens et avec de la patience et du *flair*, il serait toujours possible de déchiffrer nos dépêches sans avoir besoin d'en connaître la clé.

Il n'en sera plus de même si nous réunissons nos individus en escouades ou groupes composés d'un nombre de figures variable à volonté pourvu que notre correspondant le connaisse toujours exactement.

Supposons, pour fixer les idées, que les lettres du mot : FRANCE, soient remplacées par les personnages dont la composition est indiquée sous chaque lettre :

| F | R | A | N | C | E | + |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 3 | 2 | 1 | 1 |
| 1 | 3 | 3 | 1 | 2 | 3 | 2 |
| 1 | 1 | 3 | 1 | 1 | 2 | 1 |

Pour dérouter les recherches, nous écrirons tous nos chiffres sur une seule ligne, en faisant suivre le premier rang du second et celui-ci du troisième.

123321113312321131121.

Admettons que cette ligne représente tous nos

personnages *couchés*, chacun ayant la tête, *à gauche*, près des pieds de celui qui le précède. En les relevant, l'un après l'autre, au lieu des personnages que nous avions à l'instant, nous trouverons ceux-ci, qui correspondent aux nouvelles lettres inscrites au-dessous :

1 3 1 3 3 1 1
2 2 1 1 2 3 2
3 1 3 2 1 1 1
P L T K L Y +.

Au lieu donc d'écrire : FRANCE+, nous écrirons : PLTKLY+.

Un signe est identique et semblablement placé, dans le texte et dans le chiffre. C'est une simple coïncidence et il est facile de se rendre compte que le second + ne renferme qu'un morceau du premier, les deux autres provenant l'un de C, l'autre de E.

Pour augmenter la difficulté que présente déjà la reconstitution des lettres à qui ne connaît ni l'alphabet ni le groupement employés, nous aurions pu, avant de transformer les chiffres en lettre, faire encore coucher les *bonshommes* de notre second groupe, ce qui aurait fourni :

131331122112323132111 ;

les relevant ensuite, comme la première fois, il vient un troisième groupe dont la valeur littérale est indiquée au-dessous des chiffres :

1 3 1 1 3 1 1
3 3 2 1 2 3 1
1 1 2 2 3 2 1
Y U H M D E F

Ici, nous avons deux lettres du texte, mais ces lettres sont formées : E avec sa propre tête, suivie du corps de R et de celui de C ; F a, pour tête ses pieds, pour corps les pieds de N et enfin pour jambes les pieds de +.

En couchant, une troisième fois, nos individus fictifs et les relevant de nouveau, il viendrait :

1 1 1 2 3 1 3<br>
3 3 3 1 1 2 2<br>
1 1 3 2 1 2 1<br>
Y Y O I N H L

Encore une lettre, N, faisant partie du texte ; de quoi est-elle composée ?

Le corps de R lui sert de tête ; elle a ses propres pieds pour buste et la tête de + pour pieds ; elle ne peut donc livrer le secret du chiffre.

Reprenons la première escouade disposée sur une seule ligne :

123321113312321131121,

et, au lieu d'admettre que la tête de chacun de nos *pantins* est à *gauche,* supposons-la tournée à *droite.* Après le relèvement, il viendra :

3 1 3 2 1 1 1<br>
2 2 1 1 2 3 2<br>
1 3 1 3 3 1 1<br>
L P N S P Y +,

soit l'*inverse* de la première traduction, $L = \begin{matrix}3\\2\\1\end{matrix}$ n'étant autre chose que $P = \begin{matrix}1\\2\\3\end{matrix}$ retourné, etc.

En couchant ces nouvelles lettres pour les relever derechef, le résultat serait complètement nouveau.

Si, au lieu de *trois* images découpées en *trois* morceaux chacune, nous en prenons *cinq* coupées par la *moitié*, nous pourrons façonner, en opérant comme précédemment, *vingt-cinq* personnages divers à chacun desquels nous attribuerons une des 25 lettres de l'alphabet français.

Si nous prenons *six* personnages divisés en *deux* parties, nous en formerons *trente-six* bonshommes différents et chacun pourra être chargé de représenter une des 26 lettres (w compris) ou un des 10 chiffres arabes.

Mais cette dernière combinaison est peu pratique, du moins pour les transmissions télégraphiques. La convention internationale de Rome (14 janvier 1872) prohibant formellement, dans les dépêches chiffrées, le mélange des chiffres et des lettres, tout texte chiffré doit être composé exclusivement de lettres de l'alphabet ou exclusivement de chiffres arabes.

*
* *

Ce qui précède suffit pour faire comprendre le principe fondamental et le mécanisme de la *Cryptographie nouvelle*, laisser entrevoir les immenses ressources qu'elle présente et mettre en relief les points qui la différencient des procédés inventés jusqu'à ce jour.

---

# CRYPTOGRAPHIE NOUVELLE

---

On ne peut s'empêcher de trouver naïve la méthode employée par les empereurs César et Auguste pour tenir leur correspondance secrète. Au dire de Suétone, César remplaçait la lettre dont il avait besoin par celle qui la suivait de trois rangs dans l'alphabet, c'est-dire mettait *d* pour *a*, *e* pour *b*, *f* pour *c*, etc. Quant à Auguste, d'après le même historien, il employait *b* pour *a*, *c* pour *b*, et ainsi de suite.

Non moins naïfs les procédés usités au moyen âge, selon Raban Maur, archevêque de Mayence, qui donne deux exemples d'un système dont on se servait de son temps. Dans l'un d'eux, les voyelles sont représentées par des points : l'*i* par un point, l'*a* par deux points, l'*e* par trois, l'*o* par quatre, l'*u* par cinq, et l'on écrivait les consonnes comme à l'ordinaire.

Depuis, on a un peu perfectionné les méthodes, ou plutôt on les a compliquées, sans pour cela les rendre beaucoup plus sûres.

Le défaut capital de tous les systèmes, soit par *interversion*, soit par *substitution*, c'est d'opérer sur les lettres *entières*. Les Spartiates avaient cependant fait des tentatives dans un autre sens ; il est vrai que la *scytale* est incompatible avec le télégraphe.

On sait que, pour rendre les dépêches, qu'ils envoyaient à leurs généraux, inintelligibles à l'ennemi, dans le cas où elles seraient interceptées, les Spartiates faisaient usage de deux baguettes rondes de même diamètre et de même longueur, dont l'une était remise au général, et l'autre déposée dans les archives de l'Etat. Quand ils voulaient faire une communication au général, les magistrats prenaient leur baguette, et roulaient autour, en spirale, une étroite bande de peau, en ayant soin qu'il n'y eût aucun intervalle entre les spires. Cela fait, ils écrivaient sur cette bande, transversalement, les lignes allant d'un bout à l'autre ; puis ils la déroulaient et l'envoyaient à son adresse. Sous cette forme de lanière, la dépêche n'offrait que des lettres tronquées, en sorte que, si elle tombait entre les mains de l'ennemi, celui-ci ne pouvait la lire. Mais, lorsque le général la recevait, il l'enroulait autour de sa baguette, et les caractères revenant dans leur ordre primitif, pouvaient être facilement déchiffrés. Toute dépêche ainsi écrite s'appelait *scytale* qui signifie courroie.

Bien que ce procédé ne semble pas offrir une garantie absolue, car un chercheur, patient et sagace, pourrait, je crois, parvenir assez promptement à retrouver les parties complémentaires de quelques lettres et, par suite, la dimension de la

baguette, j'ai cru devoir appuyer un peu sur ce mode de cryptographie. C'est le seul, à ma connaissance, où les lettres soient fragmentées, le seul, par conséquent, qui ait quelque rapport avec les systèmes exposés dans le présent travail.

Laissant de côté les appareils, grilles, tableaux, codes, livres spéciaux, dictionnaires chiffrés, etc., qui présentent souvent de sérieux inconvénients et dont l'emploi ne peut être universel, je passerai également sous silence les méthodes préconisées jusqu'ici, aucune, sauf celle de Vigenère, ne me paraissant susceptible de perfectionnements suffisants pour obtenir l'impénétrabilité en même temps que la simplicité d'emploi.

Avant d'exposer les nouveaux systèmes de cryptographie, je vais indiquer les modifications à apporter au tableau de Vigenère pour en simplifier l'usage et obtenir une indéchiffrabilité presque absolue.

## 1re Méthode.

### *Tableau de Vigenère perfectionné.*

Le tableau de Vigenère est formé par un carré divisé en colonnes verticales, dont chacune porte en tête une lettre de l'alphabet placée à l'extérieur du carré; celui-ci est également séparé en bandes horizontales correspondant aux mêmes lettres disposées sur le côté du tableau.

Il renferme donc un nombre de cases égal à la deuxième puissance du nombre de lettres contenues dans l'alphabet choisi; si l'alphabet ren-

ferme 25 lettres, le nombre des cases s'élève à $25 \times 25 = 625$; si l'alphabet était de 27 lettres, il y aurait $27 \times 27 = 729$ cases.

Chaque colonne verticale, de même que chaque rangée horizontale, doit contenir toutes les lettres de l'alphabet, une par case, la même lettre ne pouvant figurer deux fois dans une même colonne ou une même rangée.

On obtient ainsi un tableau analogue à celui de la planche n° 1.

Pour se servir de ce tableau, on convient d'employer un mot-clé, *journal*, par exemple. On écrit le mot-clé sous la phrase à chiffrer, en le répétant autant de fois qu'il est nécessaire pour que chaque lettre du texte soit accompagnée d'une lettre du mot choisi. Entrant ensuite dans la table avec chacun des groupes de deux lettres ainsi formés, on prend pour lettre du chiffre celle qui appartient à la fois à la bande de l'une des lettres du groupe et à la colonne de l'autre.

Soit à traduire la phrase :

On a souvent besoin d'un plus petit que soi.

On la disposera comme suit :

On a souvent besoin d'un plus petit que soi.
JO U RNALJOU RNALJO URN ALJO URNAL JOU RNA
*rl j yljkflt ezegzl rux vask ypkqb gmn ylq*

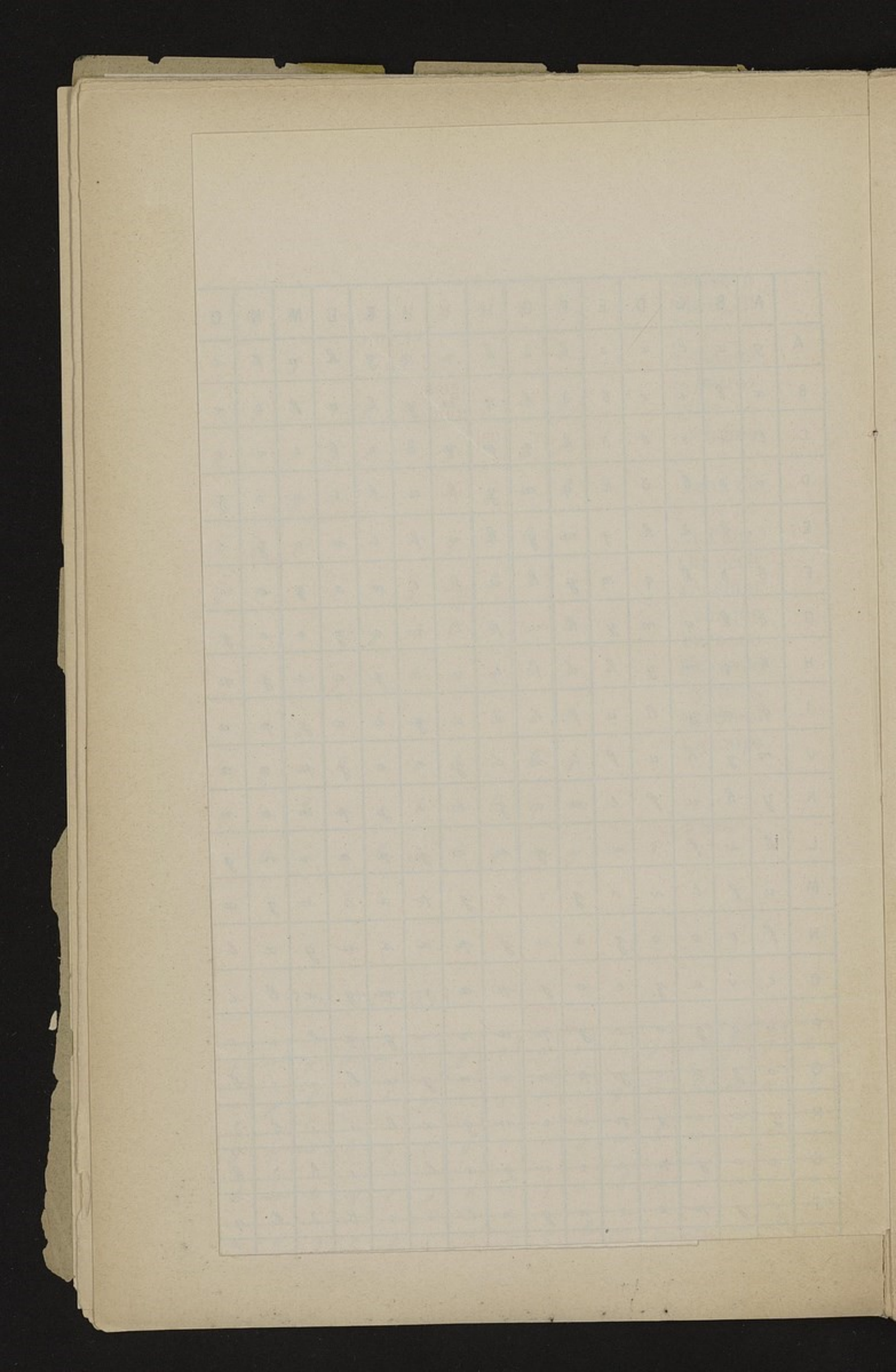
Ce qui fournit pour chiffre :

*rljyljkfltezegzlruxvaskypkqbgmnylq.*

En effet *r* se trouve dans la case commune à l'alphabet horizontal *j* et à l'alphabet vertical *o*; *l* appartient à la fois à la bande *n* et à la colonne *o*, etc. On peut, du reste, affecter indiffé-

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | g | x | l | i | s | b | d | k | q | m | y | h | u | f | t | v | o | z | e | c | j | p | a | r | n |
| B | x | l | i | s | b | d | k | q | m | y | h | u | f | t | v | o | z | e | c | j | p | a | r | n | g |
| C | l | i | s | b | d | k | q | m | y | h | u | f | t | v | o | z | e | c | j | p | a | r | n | g | x |
| D | i | s | b | d | k | q | m | y | h | u | f | t | v | o | z | e | c | j | p | a | r | n | g | x | l |
| E | s | b | d | k | q | m | y | h | u | f | t | v | o | z | e | c | j | p | a | r | n | g | x | l | i |
| F | b | d | k | q | m | y | h | u | f | t | v | o | z | e | o | j | p | a | r | n | g | x | l | i | s |
| G | d | k | q | m | y | h | u | f | t | v | o | z | e | o | j | p | a | r | n | g | x | l | i | s | b |
| H | k | q | m | y | h | u | f | t | v | o | z | e | c | j | p | a | r | n | g | x | l | i | s | b | d |
| I | q | m | y | h | u | f | t | v | o | z | e | c | j | p | a | r | n | g | x | l | i | s | b | d | k |
| J | m | y | h | u | f | t | v | o | z | e | c | j | p | a | r | n | g | x | l | i | s | b | d | k | q |
| K | y | h | u | f | t | v | o | z | e | c | j | p | a | r | n | g | x | l | i | s | b | d | k | q | m |
| L | h | u | f | t | v | o | z | e | c | j | p | a | r | n | g | x | l | i | s | b | d | k | q | m | y |
| M | u | f | t | v | o | z | e | c | j | p | a | r | n | g | x | l | i | s | b | d | k | q | m | y | h |
| N | f | t | v | o | z | e | c | j | p | a | r | n | g | x | l | i | s | b | d | k | q | m | y | h | u |
| O | t | v | o | z | e | c | j | p | a | r | n | g | x | l | i | s | b | d | k | q | m | y | h | u | f |
| P | v | o | z | e | c | j | p | a | r | n | g | x | l | i | s | b | d | k | q | m | y | h | u | f | t |
| Q | o | z | e | c | j | p | a | r | n | g | x | l | i | s | b | d | k | q | m | y | h | u | f | t | v |
| R | z | e | c | j | p | a | r | n | g | x | l | i | s | b | d | k | q | m | y | h | u | f | t | v | o |
| S | e | c | j | p | a | r | n | g | x | l | i | s | b | d | k | q | m | y | h | u | f | t | v | o | z |
| T | c | j | p | a | r | n | g | x | l | i | s | b | d | k | q | m | y | h | u | f | t | v | o | z | e |
| U | j | p | a | r | n | g | x | l | i | s | b | d | k | q | m | y | h | u | f | t | v | o | z | e | c |
| V | p | a | r | n | g | x | l | i | s | b | d | k | q | m | y | h | u | f | t | v | o | z | e | c | j |
| X | a | r | n | g | x | l | i | s | b | d | k | q | m | y | h | u | f | t | v | o | z | e | c | j | p |
| Y | r | n | g | x | l | i | s | b | d | k | q | m | y | h | u | f | t | v | o | z | e | c | j | p | a |
| Z | n | g | x | l | i | s | b | d | k | q | m | y | h | u | f | t | v | o | z | e | c | j | p | a | r |

TABLEAU N° 1.



remment les bandes ou les colonnes au mot-clé, le tableau étant symétrique.

Le déchiffrement d'une semblable dépêche ne laisse pas que d'être laborieux, car il comporte toujours un certain tâtonnement. Je ne crois pas utile de m'appesantir davantage sur ce sujet, cette méthode n'offrant pas de garanties suffisantes d'inviolabilité des dépêches, ainsi qu'il résulte des travaux de divers savants. M. Kerckhoffs a même fait connaître une méthode générale permettant de déchiffrer facilement de telles dépêches dont on ne connaît pas la clé.

Il est heureusement facile de modifier avantageusement le système de Vigenère et de lui faire acquérir une indéchiffrabilité presque absolue.

Pour cela, conservons la disposition du tableau, ainsi que les alphabets extérieurs. Le nombre des cases du carré étant égal à celui des combinaisons deux à deux des caractères contenus dans l'alphabet, nous inscrirons chacune de ces combinaisons dans l'une des cases, et nous aurons un tableau *chiffrant*, d'un emploi simple et facile.

Il suffit, en effet, de diviser la phrase à chiffrer en tranches de deux lettres, puis, se servant du tableau comme d'une table de multiplication, de remplacer chaque tranche par le groupe situé à la fois sur la bande et la colonne appartenant aux lettres du texte lues, l'une dans l'alphabet horizontal, l'autre dans l'alphabet vertical.

Il importe de remarquer que le tableau n'étant pas symétrique, il est indispensable de prendre toujours la première lettre dans le même alphabet, soit vertical, soit horizontal. Si, par exemple, nous convenons de prendre dans l'alphabet placé

à gauche du tableau la première lettre des groupes à chiffrer, et dans l'alphabet de tête la seconde lettre des mêmes groupes, l'assemblage AE sera représenté par la combinaison *(pl)* inscrite dans la 6e case de la 2e rangée, tandis que EA aura pour valeur la combinaison *(qn)* que renferme la 2e case de la 6e rangée. *(Voir le tableau n° 2.)*

Soit, par exemple, à traduire :

*On' + a' + s' ou' ve' nt' + b' es' oi' n + ' d + ' un'*
*+ p' lu' s + ' pe' ti' t + ' qu' e + ' so' i +*

On divisera cette phrase en tranches de deux lettres ; puis cherchant successivement, dans le tableau, les lettres de chaque tranche, en lisant la première dans l'alphabet vertical et la seconde dans l'alphabet horizontal, on trouvera, au point de rencontre des bandes et des colonnes, les groupes par lesquels il faut remplacer ceux du texte.

*On* se traduira donc par *gt; + a* par *gu; + s* par *ip; ou* par *iw*; *ve* par *yf;* etc., et il viendra :

*gtguipiwyfepdorasnte*
*xkwfuoxgfjdmqmnrczlwngmf.*

Remarquons que le travail de *chiffrage* est environ trois fois moindre qu'avec le tableau de Vigenère. D'abord, on n'a pas à écrire, sous chaque lettre du texte, une des lettres du *mot-clé ;* ensuite chaque recherche, dans le tableau, fournit *deux* lettres du chiffre au lieu d'*une*. Le travail est donc notablement simplifié.

D'un autre côté, l'impénétrabilité est plus grande car, tandis que dans le premier système, une lettre est remplacée par une autre, ce qui porte à 27 le nombre des valeurs qu'elle peut

| | . + | . A | . B | . C | . D | . E | . F | . G | . H | . I | . J | . K | . L | . M | . N | . O | . P | . Q | . R | . S | . T | . U | . V | . X | . Y | . Z | . W | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| +. | ix | gu | do | mq | ag | jh | sp | cf | ki | bz | yq | em | qr | kk | fp | kn | uo | ec | hj | ip | df | nc | mr | ct | di | md | ha | +. |
| A. | vb | xz | kj | yj | bq | pt | et | +d | ci | dw | xn | zl | yp | vn | hh | cc | rf | cx | ps | zy | hy | sr | ye | fb | gn | wg | ij | A. |
| B. | ck | lp | qt | be | rs | ur | cr | zh | gv | wc | hl | yn | kt | wt | mc | kh | ew | gf | sq | yt | wa | hv | fn | vo | eu | +i | gd | B. |
| C. | gi | dx | mu | ao | nh | sf | +g | wl | mm | ah | gr | b+ | hs | zu | ym | wu | rz | ey | bf | ta | +x | ld | qb | aq | v+ | qu | us | C. |
| D. | xk | km | yz | ry | f+ | tr | +t | xq | jk | +y | po | gj | jx | pe | mo | +b | uk | hw | xu | rh | ky | vi | nq | ca | lf | wy | ai | D. |
| E. | lw | qn | hp | qg | jq | +q | ob | sa | nl | px | op | vs | af | +k | xr | u+ | nt | tz | li | ra | kd | by | sl | zg | cq | jv | bp | E. |
| F. | dd | mi | ax | nb | wj | lc | zs | ie | ua | rv | s+ | tx | oy | jc | bv | tt | +n | lo | tg | rq | vz | ls | gs | yy | jl | hn | nv | F. |
| G. | kc | yk | rm | wz | oa | ov | bq | yi | xa | c+ | dk | my | nw | tq | ay | zm | rr | yb | cj | fv | on | +a | bh | tu | sz | me | kh | G. |
| H. | qa | +w | k+ | pt | to | bc | xq | lr | an | vq | +r | vp | bj | yx | fz | lz | eb | ad | wd | cl | qo | pn | bu | vw | at | qf | dq | H. |
| I. | mf | oh | tn | ux | ue | fg | qc | tb | om | du | aw | rt | xe | vy | qw | ya | +s | oz | qv | ug | pq | vh | tj | ++ | qz | xy | ou | I. |
| J. | yv | rc | wk | fm | ty | zo | ka | o+ | +e | kb | xs | dh | fy | ql | vf | uv | ok | ed | yo | pr | vg | oq | ez | dl | mz | kl | uy | J. |
| K. | hb | jf | ji | g+ | et | su | xo | vl | bo | +h | ab | +m | jz | da | +o | sw | vm | sg | um | yc | bl | vt | xd | gw | dt | yh | qe | K. |
| L. | sm | nj | pw | fe | ou | wb | dy | uj | vk | er | nf | wn | ri | sd | oe | fq | ba | np | hg | fu | sh | xg | uw | ms | pj | ho | e+ | L. |
| M. | rl | wv | ud | bn | +z | gz | i+ | tw | wp | fa | nu | pu | pp | ch | qq | dn | vi | +c | +v | lx | of | cb | se | py | gk | jy | ru | M. |
| N. | te | pb | fc | +u | rg | xp | lj | so | cd | os | la | ut | eh | xw | pg | qi | lq | dv | t+ | ro | ep | mj | fw | uf | wo | xt | gl | N. |
| O. | jg | gd | ef | vd | zn | ln | mt | rp | ia | sn | wm | jp | rb | ih | gt | po | ej | ju | uz | ni | vr | iw | ge | vv | fl | iq | zv | O. |
| P. | ws | ul | na | oo | sk | dm | yu | nn | q+ | z+ | ly | zf | ae | tv | hu | dj | ml | it | js | ar | hc | mk | xh | ei | mx | sj | lb | P. |
| Q. | ph | h+ | cv | if | bw | kw | hz | ec | zc | no | vx | re | jm | ti | ea | ht | ww | mn | +l | tm | bb | cz | ir | yd | uh | iy | in | Q. |
| R. | wq | es | ol | ja | xi | qk | ap | nd | ds | ll | zk | zq | m+ | gb | ys | ns | og | fs | gp | bd | ik | mw | fi | we | dc | cp | tf | R. |
| S. | fj | eg | zr | zw | lm | mv | ce | kq | lt | tk | pz | pd | ev | l+ | oi | ng | +f | br | aw | ub | zi | ke | tc | yw | za | gy | ko | S. |
| T. | nr | cs | ig | sv | x+ | n+ | rw | fr | yr | qm | iv | si | wr | qs | ib | kd | vj | gm | de | wx | fo | gx | pm | fk | jd | eq | mg | T. |
| U. | eo | fh | ss | xl | mb | id | nx | is | qy | zj | lg | dp | pa | kr | wf | +p | zt | r+ | be | cw | nk | zx | jo | ic | jw | or | lv | U. |
| V. | cy | ze | a+ | xm | oc | yf | jn | jt | iu | mp | tp | lh | kg | kp | am | bx | hk | hi | ot | ek | ku | y+ | ox | qj | im | ft | hx | V. |
| X. | td | gh | yg | dg | kv | il | wi | lu | pv | rd | zb | d+ | uc | vc | aj | kf | ne | hf | en | jj | nz | dr | zz | wb | iz | aa | nm | X. |
| Y. | vu | io | gq | ks | qx | av | ve | xb | kz | gg | ac | ga | zd | cn | bk | jr | al | +j | th | rn | bs | pf | j+ | hm | fx | db | sx | Y. |
| Z. | pi | sy | xj | qh | yl | va | pk | ex | bg | st | ui | rj | ak | go | od | je | w+ | rk | sb | ff | up | em | ow | uu | as | xv | sc | Z. |
| W. | zp | bt | le | bi | hr | rx | un | az | xx | xf | fd | jb | cg | oj | lk | ny | mh | wq | tl | p+ | bm | co | ma | ts | dz | gc | qp | W. |
| | . + | . A | . B | . C | . D | . E | . F | . G | . H | . I | . J | . K | . L | . M | . N | . O | . P | . Q | . R | . S | . T | . U | . V | . X | . Y | . Z | . W | |

TABLEAU N° 2.

prendre, dans le nouveau système, le nombre des combinaisons étant de 27 × 27 = 729, chaque groupe peut avoir 729 valeurs différentes.

Nous pouvons aller plus loin. Ainsi, au lieu de grouper les lettres deux à deux et de les traduire dans l'ordre qu'elles occupent, séparons-les en groupes quelconques ; écrivons le deuxième groupe sous le premier, le quatrième sous le troisième, et ainsi de suite. Si le dernier groupe est incomplet, on rendra d'abord, s'il y a lieu, pair le nombre des lettres contenues dans les deux derniers groupes ; puis, séparant le tout en deux parties égales, on écrira la seconde moitié sous la première.

Proposons-nous de chiffrer la phrase qui précède, en la groupant par *six*. Nous aurons :

| | | | |
|---|---|---|---|
| *on+a+s* | *+besoi* | *+plus+* | *que+* |
| *ouvent* | *n+d+un* | *petit+* | *soi+* |

Le travail ainsi disposé, on cherche dans le tableau les groupes que forment les lettres supérieures et inférieures et l'on écrit au-dessous la combinaison qui correspond à chacune d'elles, c'est-à-dire *pc* au lieu de *oo; mj* pour *nu ; mr* pour *+v*, etc., comme ci-dessous :

| | | | |
|---|---|---|---|
| *on+a+s* | *+besoi* | *+plus+* | *que+* |
| *ouvent* | *n+d+un* | *petit+* | *soi+* |
| *pmmpfz* | *fcjfiq* | *udszzi* | *t+pi* |
| *cjrlpi* | *pkqjww* | *omhjix* | *mpxx* |

Ecrivant ensuite les lettres du chiffre en faisant suivre les six premières lettres de chaque groupe des six dernières lettres, il vient :

*pmmpfzcjrlpifcjfiqpkqjwwudszziomhjixt+pi mpxx.*

Ici, rien n'indique plus la composition des groupes et chaque lettre du groupe représente, non une lettre du texte, mais la moitié de la combinaison correspondant à un groupe de deux lettres prises dans deux endroits du texte. En considérant que chaque lettre entre dans $54 = 2 \times 27$ assemblages différents, on voit facilement qu'elle peut avoir $54 \times 54 = 2{,}916$ valeurs diverses.

S'il est facile de chiffrer, il est tout aussi facile de traduire. Le travail est exactement le même ; il faut seulement se servir du tableau *déchiffrant*, qui est l'inverse du premier. Cependant on peut composer des tableaux *réciproques*, en prenant pour représenter un groupe de lettres le groupe qu'il représente lui-même : ainsi *pm* étant représenté par *tv*, *tv* sera réciproquement représenté par *pm*. Le même tableau sert alors indifféremment à *chiffrer* ou à *déchiffrer*. C'est le cas du tableau ci-joint.

On veut traduire la phrase :

*geikjupzal'tpxjhbcjmw'ujnodwnzmi'khksfspx vx'tjkg,*

que l'on sait avoir été groupée par *dix*.

On opérera comme suit :

| | | |
|---|---|---|
| *ge i k j upz a l* | *u j nodwnzm i* | *tj* |
| *tpx j h b c jmw* | *k h ks f s pxv x* | *kg* |
| *on+a+sou v e* | *d+un+p l u s+* | *so* |
| *n t+b e so i n+* | *p e t i t+que+* | *i+* |

En rapprochant les trois chiffres ci-dessus, qui, tous les trois, représentent la même phrase, on

reconnaît facilement qu'ils sont absolument dissemblables, bien que formés à l'aide du même tableau. Cela montre bien l'importance du *groupement*, et prouve que, si l'indéchiffrabilité est absolue pour qui ne possède pas le tableau, elle est presque aussi grande pour le chercheur muni du tableau mais ignorant le chiffre du groupement.

Le groupement peut, du reste, être modifié à volonté ; il n'a d'autres limites que la fantaisie des correspondants : il peut être régulier, comme dans les chiffres ci-dessus, ou irrégulier, par exemple, en formant le premier groupe de 8 lettres, le second de 5, le troisième de 13....; la première ligne de chaque groupe peut être mise au second rang; les groupes peuvent enfin être mêlés de toutes façons. Il suffit pour chiffrer clairement et pour traduire correctement, que les *conventions* soient bien établies.

Je ne m'appesantirai pas davantage sur ce système, malgré les avantages réels qu'il présente sur les méthodes analogues, car il a l'inconvénient grave de nécessiter l'emploi d'un tableau. Ce tableau, dont la confection ne laisse pas d'être laborieuse, ne peut être modifié sans un travail long et pénible, si toutefois on tient à conserver la *réciprocité* des combinaisons.

Il importait donc de trouver une méthode offrant tous les avantages de celle qui vient d'être exposée, et cela sans qu'on soit astreint à se servir d'un document dont l'absence empêche toute correspondance secrète et dont la possession par un tiers peut avoir de graves conséquences, surtout pour une armée en campagne.

Le système que j'ai dénommé *militaire* pare à tous ces inconvénients, ainsi qu'on le verra plus loin.

Cependant, avant d'exposer ce système, je crois qu'il est bon de faire connaître le principe essentiel de la nouvelle cryptographie et son application au service *diplomatique* ou commercial.

## 2e MÉTHODE

### *Système diplomatique.*

La base de la méthode consiste à composer un vocabulaire renfermant : 1° toutes les lettres de l'alphabet plus les signes de ponctuation ou autres nécessaires pour la clarté de la correspondance ; 2° les mots ou phrases les plus usuels.

A chaque article de ce vocabulaire, lettre, mot ou phrase, on attribue un nombre de deux ou trois chiffres ; de deux chiffres si on peut se contenter de 99 articles et de trois chiffres dans le cas contraire. On dispose alors de 999 numéros.

Comme il est indispensable que chaque article soit représenté par un même nombre de chiffres, au lieu de 1, 2, 3...., on écrit, suivant le cas, 01, 02, 03...., ou 001, 002, 003.... Le double ou triple zéro, 00, 000, ne doit rien représenter ; il n'a donc aucune valeur dans les dépêches où il figure. On en verra plus loin la raison.

Le vocabulaire établi, on dresse un petit tableau, dans lequel auprès de chacun des dix chiffres on écrit deux des lettres de l'alphabet normal. Les

cinq ou six lettres complémentaires sont attribuées aux signes de calcul usités en arithmétique.

Les accessoires ainsi formés, pour chiffrer une dépêche, on remplace, suivant le cas, la lettre, le mot ou la phrase à transmettre par le nombre qui lui correspond, dans le vocabulaire. On obtient ainsi une série de chiffres que l'on groupe, suivant les conventions, d'une manière analogue à celle expliquée dans la méthode précédente. On effectue ensuite, sur chaque groupe de chiffres, une addition, une soustraction ou, en général, un calcul quelconque, qui a pour résultat de modifier tous les chiffres et de leur substituer des nombres n'ayant aucun rapport avec les premiers.

Supposons, pour fixer les idées, qu'il s'agisse de chiffrer la dépêche suivante :

*Monsieur, attendez l'arrivée de M. Lucien, qui vous remettra une lettre de crédit d'une valeur de 257 livres sterling sur la maison Gibson frères, de Chicago. Il y joindra des instructions sur la vente de vos marchandises et l'achat des machines, au mieux de nos intérêts. Avisez-nous par télégramme de votre départ.*

Pour cela, nous nous servirons du vocabulaire ci-contre, dont notre correspondant possède la copie :

| | | |
|---|---|---|
| 00 — pas de valeur | 19 — s | 52 — par |
| 01 — a | 20 — t | 53 — sur |
| 02 — b | 21 — u | 55 — une |
| 03 — c | 22 — v | 63 — achat |
| 04 — d | 23 — x | 64 — arrivée |
| 05 — e | 24 — y | 67 — avisez-nous |
| 06 — f | 25 — z | 68 — départ |
| 07 — g | 26 — w | 72 — frères |
| 08 — h | 27 — + | 74 — instructions |
| 09 — i | 28 — [ ] | 76 — machines |
| 10 — j | 30 — et | 78 — maison |
| 11 — k | 31 — de | 81 — marchandises |
| 12 — l | 32 — des | 83 — monsieur |
| 13 — m | 35 — la | 87 — lettre de crédit d'une valeur de |
| 14 — n | 37 — il | 89 — livres sterling |
| 15 — o | 39 — vos | 90 — télégramme |
| 16 — p | 40 — votre | 93 — vente |
| 17 — q | 41 — vous | 95 — au mieux de nos intérêts |
| 18 — r | 46 — qui | |

*Nota.* — Le signe +, n° 27, sert à séparer les mots et à indiquer la ponctuation; la parenthèse, n° 28, se met avant et après les nombres écrits en chiffres; il est bon que ces derniers soient en nombre pair, ce que l'on obtient facilement par l'adjonction d'un zéro, quand il y a lieu.

Maintenant, chiffrons, ce qui se fera simplement en remplaçant chaque mot ou lettre par le nombre voisin et en écrivant tous les chiffres à se suivre. *Monsieur* sera représenté par 83; *attendez* n'étant pas prévu au vocabulaire, s'écrira lettre par lettre, en mettant pour *a*... 01, pour *t*... 20..., etc.

Nous obtiendrons ainsi le *chiffre* suivant :

8327012020051404052527122764318327122103090 514464118051305202018015587280257288953357807 090219151472310308090301071527273724101509140 418013274533593313981301227633276952727675:90 314068.

Si nous craignons que cette dépêche soit interceptée par une personne munie de notre vocabulaire, il nous est aisé d'obtenir des garanties nouvelles de sécurité. Il nous suffit, soit d'ajouter ou de retrancher un *nombre-clé*, soit d'opérer un calcul quelconque connu de notre correspondant ou indiqué dans la dépêche même.

Plus simplement encore, divisons notre nombre par groupes, de cinq par exemple, en écrivant le second sous le premier, le troisième au-dessous, etc., comme ceci :

| | | | |
|---|---|---|---|
| 83270 | 76431 | 18051 | 72889 |
| 12020 | 83271 | 30520 | 53357 |
| 05140 | 22103 | 20180 | 80709 |
| 40525 | 09051 | 15587 | 02191 |
| 27122 | 44641 | 28025 | 51472 |

etc., etc.

Il est évident que, si nous transmettons les tranches verticales successives, notre correspondant, prévenu, n'aura nulle dificulté à retrouver l'ordre des chiffres. Au lieu de lire : 810423250720 1517242200052..., il écrira verticalement les cinq premiers chiffres, mettra à côté les cinq suivants et ainsi de suite ; la traduction sera alors facile.

Au lieu d'écrire l'un auprès de l'autre les chiffres

du vocabulaire, on peut encore les superposer, de manière à scinder les numéros des signes, comme suit :

8202201002212638212O . . . . . . . . . . . .
3710054455727413721З . . . . . . . . . . . .

Il est inutile de dire que les nombres, ainsi obtenus, sont à leur tour susceptibles d'être modifiés par des calculs de toute sorte.

Il nous reste à convertir en lettres les chiffres, modifiés ou non, intervertis ou non. Ce résultat sera facilement atteint à l'aide d'un tableau analogue à celui-ci :

| | | | |
|---|---|---|---|
| 0 — e, g | a = 1 | n = 8 | Lettres-signes |
| 1 — a, b | b = 1 | o = 3 | h = +, plus |
| 2 — i, d | c = 9 | p = 4 | j = —, moins |
| 3 — o, m | d = 2 | q = 5 | k = ×, multipliez |
| 4 — u, p | e = 0 | r = 6 | x = : divisez |
| 5 — y, q | f = 7 | s = 7 | z — indique la fin |
| 6 — r, v | g = 0 | t = 8 | d'un calcul et |
| 7 — s, f | i = 2 | u = 4 | le commence- |
| 8 — t, n | l = 9 | v = 6 | ment d'un |
| 9 — c, l | m = 3 | y = 5 | autre. |

Appliquons cette nouvelle clé aux vingt-cinq premiers chiffres de notre dépêche, groupés par cinq et lus verticalement. Il viendra

*Taguimdyesiebyasipidegeyd*. . .,

assemblage de lettres qui n'ont, certes, aucun rapport avec le texte primitif et qui peuvent être diversifiées à volonté, chaque chiffre pouvant être indifféremment traduit par deux lettres différentes.

On pourrait, par suite, représenter le même nombre par

*Nbepdoiqgfdgaqbfdudigegqi...*

ou par

*Nagudodygs gbqbsiuiigggyd...*

ou par tout autre assemblage de lettres ayant la même valeur numérique.

Il convient maintenant de faire connaître l'emploi des *lettres-signes* et la raison du rejet de *oo* comme signe chiffrant.

*Méthode des sommes et différences.* -- Supposons que les conventions établies entre deux correspondants, possesseurs du même vocabulaire, soient les suivantes :

Ecrire les *numéros* verticalement, le premier chiffre à la ligne supérieure, le second à la ligne inférieure. Diviser en groupes de *cinq* ou *six* numéros. Faire successivement, pour chaque groupe, la somme et la différence des deux nombres qui le composent, en ayant soin de laisser toujours le nombre le plus fort à sa place relative, c'est-à-dire de commencer par l'*addition*, quand le *plus grand nombre* est à la ligne supérieure, et par la *soustraction* quand il se trouve à la seconde ligne.

La *somme* devant avoir *six* chiffres, le groupe ne peut renfermer que *cinq* numéros, lorsque l'addition des deux premiers chiffres surpasse dix. Les chiffres manquants, à la différence, sont remplacés par des zéros.

Le résultat des calculs, converti en lettres, est ensuite expédié en écrivant le second nombre de

chaque groupe immédiatement après le premier.

Ceci établi, voyons en quoi consiste le déchiffrement.

Ayant reçu la dépêche suivante :

*Bacaidepulidyouqoyqypyflausfyqpegyacelocym omolqygafsydbeqlyu......*

Nous remplaçons les lettres par les chiffres qui leur correspondent et que nous séparons par tranches de *six*, comme suit :

| | | | | |
|---|---|---|---|---|
| 119122 | 044922 | 534535 | 554579 | 147755 |
| 400519 | 093953 | 333955 | 017752 | 105954.... |

écrivant ensuite les groupes de rang pair sous ceux de rang impair, qui les précèdent, nous ferons successivement la somme et la différence de ces quantités, en tenant compte de la convention relative à la place occupée par le nombre le *plus fort*. Il ne nous restera plus qu'à prendre la moitié de chaque nombre, à rejeter les *colonnes de zéros*, que le calcul a pu introduire, et, enfin, à chercher, dans le vocabulaire, la valeur de chaque tranche verticale.

Voici la disposition du travail :

| | |
|---|---|
| 119122 | 534535 |
| 044922 | 554579 |
| 164044 : 2 = 82022 | 020044 : 2 = 010022 |
| 074200 : 2 = 37100 | 1089114 : 2 = 544557 |
| | |
| 147755 | 093953 |
| 400519 | 333955 |
| 252764 : 2 = 126382 | 240002 : 2 = 120001 |
| 548274 : 2 = 274137 | 427908 : 2 = 213954 |

017752
105954

088202 : 2 = 44101
123706 : 2 = 61853

et nous retrouvons le nombre que nous connaissons déjà :

8202201002212638212000144101
3710054455727413721395461853

*Méthode des différences successives.* — Ici les opérations à effectuer sont indiquées par les *lettres-signes.* Nous recevons, par exemple, une dépêche qui, traduite en chiffres, devient :

22407 + 4375 + 498 + 74.

Nous disposons alors le travail de la manière suivante :

| | | | |
|---|---|---|---|
| 22407 | | | |
| | + 4375 | | |
| 26782 | | + 498 | |
| | + 4873 | | + 74 |
| 31655 | | + 572 | |
| | + 5445 | | |
| 37100 | | | |

Il semble inutile de détailler la marche du calcul, qui reproduit, comme l'on voit, le commencement de la seconde ligne du chiffre ci-dessus :

37100544557274.

L'infinie variété des calculs auxquels se prêtent les nombres assure l'indéchiffrabilité absolue à tout système, tel que vocabulaire numéroté, dictionnaire chiffré, code numérique, etc., permettant de transformer une dépêche en nombres arithmétiques.

Mais, à côté de cet avantage, existe l'inconvénient de recourir à des livres ou tableaux spéciaux et d'effectuer des calculs et des transpositions, qui peuvent être faciles dans un bureau, mais sont absolument impraticables pour une armée en marche et surtout en campagne.

Heureusement que l'application des principes exposés dans les méthodes ci-dessus va nous conduire à un nouveau système présentant tous les avantages des deux premiers, sans en avoir les inconvénients.

Nous avons vu, dans la première méthode, qu'il est facile de scinder un groupe de signes, d'en mélanger les fragments presque sans travail pour ainsi dire mécaniquement, et de les retrouver avec la même facilité.

Dans la deuxième méthode, nous avons appris à transformer nos phrases en remplaçant le texte primitif par des chiffres qui, à leur tour, sont remplacés par des lettres. Nous avons, en outre, remarqué qu'il importe peu qu'on nous transmette un tableau de chiffres ou de lettres par tranches horizontales ou par tranches verticales, du moment que nous connaissons la position exacte à donner à chaque tranche.

Tels sont les trois principes sur lesquels est basé le système de cryptographie *militaire*.

### 3e Méthode

### *Système militaire.*

Imitons le procédé des Spartiates ; brisons nos lettres en plusieurs fragments ; mélangeons ces fragments ; puis réunissons-les en nombre conve-

nable pour reproduire de nouvelles lettres. Ces lettres constitueront notre cryptogramme.

A la réception, elles seront brisées à leur tour et reproduiront, dans un ordre voulu, les fragments des premières, qui pourront alors être reconstituées.

Pour fragmenter une lettre, il faut la représenter par une combinaison de signes ; les plus simples étant les chiffres, c'est de ceux-ci que nous ferons exclusivement usage.

Nous attribuerons donc à chaque lettre un nombre, ou groupe de plusieurs chiffres. Mais, s'il est indispensable que chaque lettre soit représentée par un groupe différent, c'est-à-dire qu'il y ait autant de combinaisons de chiffres que de lettres, il est tout aussi indispensable qu'il y ait autant de lettres que de combinaisons. S'il en était autrement, une combinaison produite par la fragmentation des groupes pourrait ne pas se trouver représentée et le chiffrage deviendrait impossible.

Cette nécessité inéluctable limite le nombre de chiffres à donner à chaque lettre.

En effet, le nombre de *combinaisons* que l'on peut former avec $x$ objets groupés $n$ à $n$ de toutes les manières possibles, est égal à

$$C_n = X^n \ ;$$

c'est-à-dire que 3 objets, par exemple, groupés deux à deux, fournissent $9 = 3^2$ combinaisons, ainsi $a, b, c$, donnent $aa, ab, ac, ba, bb, bc, ca, cb, cc$.

De même, 5 objets groupés deux à deux fourniront $5^2 = 25$ combinaisons ; 4 objets n'en auront que 16 et 6 en auraient 36.

Il en résulte que, pour un alphabet de 25 lettres, les combinaisons à employer seront fournies par *cinq* chiffres groupés *deux à deux*.

En faisant, dans la formule ci-dessus, $x = 3$ et $n = 3$, nous trouverons

$$C_3 = 3^3 = 27.$$

Donc, en ajoutant à l'alphabet usuel le *w* et le signe +, qui nous servira à séparer les mots et les phrases, nous pourrons employer les combinaisons fournies par *trois* chiffres groupés *trois* à *trois*.

Nous aurons ainsi la faculté de scinder nos lettres, à notre choix, en *deux* ou en *trois* fragments.

On verra plus loin qu'il est même possible de les diviser en *quatre*, *six*, *neuf*, etc., parties.

Venons à l'application et formons d'abord un alphabet. Pour plus de simplicité, je laisserai les lettres et les combinaisons dans leur ordre naturel. L'alphabet sera donc, à la fois, *chiffrant* et *déchiffrant*.

| | | | | |
|---|---|---|---|---|
| a = 11 | f = 21 | k = 31 | p = 41 | u = 51 |
| b = 12 | g = 22 | l = 32 | q = 42 | v = 52 |
| c = 13 | h = 23 | m = 33 | r = 43 | x = 53 |
| d = 14 | i = 24 | n = 34 | s = 44 | y = 54 |
| e = 15 | j = 25 | o = 35 | t = 45 | z = 55 |

Pour chiffrer, il faut écrire le texte en espaçant un peu les lettres ; écrire ensuite *verticalement*, sous chacune d'elles, le nombre qui lui correspond, dans l'alphabet ; séparer, par un trait vertical, ou de toute autre manière, le nombre de lettres convenu avec le destinataire ; puis, lisant

les chiffres *deux* à *deux* et *horizontalement*, chercher, dans l'alphabet, la lettre correspondante, que l'on écrit sous les chiffres. Après avoir remplacé par leur valeur *littérale* les chiffres de la première ligne de *chaque groupe*, on traduit de même la seconde ligne, puis l'on passe au groupe suivant. On opère toujours comme si la seconde ligne de chaque groupe était écrite à la suite de la première. Lors donc qu'il reste un chiffre à la fin de la première ligne, on le considère comme placé devant le premier chiffre de la deuxième ligne, ce qui se fait sans aucune difficulté.

D'après cela, pour traduire :

Un soldat doit être courageux,

en groupant par *cinq*, on opérera ainsi :

| | | | | |
|---|---|---|---|---|
| u n s o l | d a t do | i t ê t r | e c o u r | a g e u x |
| 5 3 4 3 3 | 1 1 4 1 3 | 24 14 4 | 1 1 3 5 4 | 1 2 1 5 5 |
| 1 4 4 5 2 | 4 1 5 45 | 45 55 3 | 5 3 5 1 3 | 1 2 5 1 3 |
| XRKSV | APNET | IDSZX | AOTOC | BEUJC |

et on aura le chiffre :

*xrksvapnetidszxaotocbeujc*,

qui ne semble pas avoir le moindre rapport avec la phrase proposée.

Analysons le travail effectué pour l'obtenir. Après avoir écrit la phrase donnée, en espaçant les lettres, nous avons séparé les groupes composés, suivant nos conventions, de *cinq* lettres chacun. Cherchant ensuite dans l'alphabet, nous avons trouvé 51 pour la valeur numérique de *u*, 34 pour celle de *n*, 44 pour *s*, 35 pour *o*, 32 pour *l*, etc., etc., soit, pour le premier groupe : u = 51,

n = 34, s = 44, o = 35, l = 32. Ecrivant tous ces nombres *verticalement* sous les lettres qu'ils représentent, nous avons formé le tableau suivant :

| | | | | |
|---|---|---|---|---|
| *u* | *n* | *s* | *o* | *l* |
| 5 | 3 | 4 | 3 | 3 |
| 1 | 4 | 4 | 5 | 2 |

Relevant ensuite le premier chiffre de *u*, ou 5, et le premier de *n*, 3, nous lisons 53, nombre qui, dans l'alphabet, correspond à *x* ; en associant le premier chiffre de *s* avec le premier de *o*, il vient 43, qui représente *r* ; le premier chiffre de *l* combiné au deuxième de *u* donne 31 ou *k* ; les deuxièmes chiffres de *n* et de *s* fournissent le nombre 44, soit *s* ; et, enfin, les derniers chiffres de *o* et de *l* donnent 52, dont la valeur est *v*.

En résumé, nous avons :

53 = x ; 43 = r ; 31 = k ; 44 = s ; 52 = v ;

le premier groupe se traduira donc par

xrksv.

Le travail est exactement le même pour les autres groupes ; il est donc sans intérêt d'insister, les détails qui précèdent indiquant suffisamment la marche de l'opération.

Il est bon de faire remarquer que, en groupant les lettres par nombre *pair*, deux lettres voisines, dont la première est de rang impair, sont toujours représentées par les deux mêmes lettres, comme dans le tableau de Vigenère perfectionné.

Ainsi *u n*, ayant pour valeurs numériques *u* = 51 et *n* = 34, reproduiront toujours dans ce cas les deux nombres 53 et 14, qui représentent *x*

et $d$ ; $s = 44$ et $o = 35$ donneront $43 = r$ et $45 = t$ ; $l = 32$ et $d = 14$ fourniront toujours $31 = k$ et $24 = i$ ; et ainsi des autres.

Il n'en est plus de même lorsqu'on choisit un nombre *impair* pour base du groupement. Alors la première moitié de $u$ s'associe encore à la première de $n$ pour donner $53 = x$ ; mais la seconde moitié de $u$ se joindra à la première de $s$, si la base du groupement est *trois*, à la première de $l$, si cette base est *cinq*, à la première de $a$, si cette base est *sept*, etc. Dans le premier cas, on aura la combinaison $41 = p$ ; dans le second, $31 = k$ ; dans le troisième, $11 = a$ ; .... L'opération du chiffrage n'est pas plus laborieuse et la sécurité est grandement augmentée, puisque les deux moitiés de chaque lettre sont absolument disjointes.

Il est intéressant de rechercher la composition des lettres du chiffre ; mais, afin de pouvoir faire ressortir, en même temps, l'influence du *groupement*, nous allons de nouveau chiffrer notre phrase, en groupant par des nombres différents, par *sept* et par *trois*.

En groupant par *sept*, on trouve :

| | | | |
|---|---|---|---|
| u n s o l d a | t d o i t e t | r e c o u r a | g e u x |
| 53.43.31.1 | 41 32.41.4 | 41.13.54.1 | 21.55. |
| 1.44.52.41. | 5.45.45.55. | 3.53.51.31. | 25.13. |
| XRKASVP | PLPTTTZ | PCYCXUK | FZJC |

En groupant par *trois,* il vient :

| | | | | | |
|---|---|---|---|---|---|
| u n s | o l d | a t d | o i t | e t r | e c o |
| 53.4 | 33.1 | 14.1 | 32.4 | 14.4 | 11.3 |
| 1.44. | 5.24. | 1.54. | 5.45. | 5.53. | 5.35. |
| XPS | MEI | DAY | LTT | DTX | AOO |

| | | |
|---|---|---|
| u r a | g e u | x |
| 54.1 | 21.5 | 5 |
| 1.31. | 2.51. | 3 |
| YAK | FVU | X |

Cherchons maintenant la valeur des lettres de chaque *chiffre*, en fonction des lettres du texte. Pour abréger l'écriture, je représenterai par $u_1$, $n_1$. $s_1$,... la *première partie* de *u*, *n*, *s*..., et par $u_2$, $n_2$, $s_2$,... la *seconde* partie des mêmes lettres. De cette façon, X = $u_1\,n_1$ signifiera que X a été formé en faisant suivre le premier chiffre de *u* du premier chiffre de *n*; P = $s_1\,u_2$ indiquera que P est composé du premier chiffre de *s* suivi du deuxième de *u*; etc.

| Groupement par | 3 | 5 | 7 |
|---|---|---|---|
| 1re lettre du chiffre | X = $u_1\,n_1$ | X = $u_1\,n_1$ | X = $u_1\,n_1$ |
| 2e — | P = $s_1\,u_2$ | R = $s_1\,o_1$ | R = $s_1\,o_1$ |
| 3e — | S = $n_2\,s_2$ | K = $l_1\,u_2$ | K = $l_1\,d_1$ |
| 4e — | M = $o_1\,l_1$ | S = $n_2\,s_2$ | A = $a_1\,u_2$ |
| 5e — | E = $d_1\,o_2$ | V = $o_2\,l_2$ | S = $n_2\,s_2$ |
| 6e — | I = $l_2\,d_2$ | A = $d_1\,a_1$ | V = $o_2\,l_2$ |
| 7e — | D = $a_1\,t_1$ | P = $t_1\,d_1$ | P = $d_2\,a_2$ |
| 8e — | A = $d_1\,a_2$ | N = $o_1\,d_2$ | P = $t_1\,d_1$ |
| 9e — | Y = $t_2\,d_2$ | E = $a_2\,t_2$ | L = $o_1\,i_1$ |
| 10e — | L = $o_1\,i_1$ | T = $d_2\,o_2$ | P = $t_1\,e_1$ |
| 11e — | T = $t_1\,o_2$ | I = $i_1\,t_1$ | T = $t_1\,t_2$ |
| 12e — | T = $i_2\,t_2$ | D = $e_1\,t_1$ | T = $d_2\,o_2$ |
| 13e — | D = $e_1\,t_1$ | S = $r_1\,i_2$ | T = $i_2\,t_2$ |
| 14e — | T = $r_1\,e_2$ | Z = $t_2\,e_2$ | Z = $e_2\,t_2$ |
| 15e — | X = $t_2\,r_2$ | X = $t_2\,r_2$ | P = $r_1\,e_1$ |

En étudiant ce tableau, qu'il ne semble pas utile de poursuivre plus loin, on voit d'abord que,

quand une lettre possède la même valeur dans des groupements différents, ce n'est que par exception qu'elle occupe le même rang. Ainsi, S = $n_2 s_2$ est la 3[e] lettre dans le groupement par 3, la 4[e] dans le groupement par 5, et la 5[e] dans celui par 7 ; de même, V = $o_2 l_2$ occupe la 5[e] place dans la seconde colonne, et la 6[e] dans la dernière ; P = $t_1 d_1$ est au 7[e] rang dans la 2[e] colonne, et au 8[e] dans la troisième.

En outre, la même lettre, dans un même chiffre ou dans des chiffres différents, se reproduit rarement avec la même valeur. Nous voyons, par exemple, dans le groupement par *sept*, P figurer quatre fois et représenter successivement $d_2\,a_2$, $t_1\,d_1$, $t_1\,e_1$, $r_1\,e_1$ ; T figure trois fois et a pour valeurs $t_1\,t_2$, $d_2\,o_2$, $i_2\,t_2$.

Il est facile de calculer le nombre des combinaisons qui peuvent amener une lettre déterminée. Soit P cette lettre ; sa valeur, dans notre alphabet, est 41. Cinq lettres ont 4 pour premier chiffre, ce sont *p*, *q*, *r*, *s*, *t* ; cinq lettres ont également 4 pour second chiffre, *d*, *i*, *n*, *s*, *y*. Le 4 de 41 peut donc être donné indifféremment par les dix moitiés de lettres que nous désignons par $p_1$, $q_1$, $r_1$, $s_1$, $t_1$, $d_2$, $i_2$, $n_2$, $s_2$, $y_2$. De même, le 1, second chiffre de 41, peut provenir de $a_1$, $b_1$, $c_1$, $d_1$, $e_1$, $a_2$, $f_2$, $k_2$, $p_2$, $u_2$. Or, chacun des symboles de la première série peut être suivi de l'un quelconque des symboles de la deuxième série ; le nombre total des combinaisons de lettres susceptibles de fournir 41, valeur de P, est égal à $10 \times 10 = 100$. Il convient, en outre, de remarquer que les lettres, qui concourent à former cette valeur, sont tantôt rapprochées et tantôt plus ou moins éloignées, ce qui

augmente encore la difficulté du déchiffrement *sans clé*.

Pour traduire une phrase chiffrée, on écrit *horizontalement* les nombres correspondant à chaque lettre d'un même *groupe ;* on sépare ensuite les chiffres obtenus en deux parties égales et on reproduit les chiffres de la seconde moitié sous ceux de la première. Il ne reste plus qu'à lire les nombres *verticalement* et à écrire au-dessous de chacun d'eux la lettre qui les représente dans l'alphabet.

Soit proposé de traduire :

KGCUTZOJYAPSYDTPHNTS,

sachant qu'on a *groupé* alternativement par *cinq* et par *trois*.

Les *cinq* premières lettres, ayant pour valeurs : K = 31, G = 22, C = 13, U = 51, T = 45, nous donneront le nombre

31221'35145

que nous divisons en deux tranches de *cinq* chiffres et écrivons

31221
35145

en reportant la seconde tranche sous la première.

Avec un peu d'attention, à défaut d'habitude, on écrit du premier coup les chiffres les uns sous les autres. On est guidé, dans cette opération, par le nombre des lettres de chaque groupe, en ayant soin de mettre d'abord un seul chiffre sous chaque lettre. Il est bon d'avoir soin de pointer les lettres

au fur et à mesure qu'on les transforme en chiffres ; cette petite précaution fera éviter bien des erreurs.

Voici l'opération entière :

| | | | | |
|---|---|---|---|---|
| . . . . . | . . . | . . . . . | . . . | . . . . |
| KGCUT | ZOJ | YAPSY | DTP | HNTS |
| 3 1 2 2 1 | 5 5 3 | 5 4 1 1 4 | 1 4 4 | 2 3 3 4 |
| 3 5 1 4 5 | 5 2 5 | 1 4 4 5 4 | 5 4 1 | 4 5 4 4 |
| m e f i e | z v o | u s d e s | e s p | i o n s |

Ce qui précède est amplement suffisant pour faire connaître la méthode. Quant au changement d'alphabet et aux divers modes de groupement, on trouvera plus loin des renseignements détaillés, qu'il est inutile de donner ici.

L'alphabet à *trois* chiffres ne différant pour ainsi dire pas de celui à *deux* chiffres, quant à la manière d'opérer, je ne reproduirai pas les détails minutieux dans lesquels je suis entré. Le lecteur en sera quitte pour se reporter aux pages précédentes, s'il rencontre quelque difficulté.

Nous savons que trois objets, pris trois à trois, peuvent se grouper de $3^3 = 27$ manières différentes ; en d'autres termes, trois mêmes chiffres forment 27 nombres différents, compris entre 100 et 1000.

D'autre part, l'alphabet usuel, augmenté de W et du signe +, se compose de 27 caractères. Il est donc possible d'attribuer une lettre à chaque combinaison numérique, et réciproquement une de ces combinaisons à chaque lettre.

Prenons les chiffres les plus simples, 1, 2 et 3, puis groupons-les, *trois à trois*, de toutes les façons

possibles. Auprès de chaque groupe, plaçons une des lettres de l'alphabet et nous aurons tout ce qu'il faut pour écrire un cryptogramme.

Il est utile, pour faciliter le chiffrage, d'établir deux alphabets, l'un *chiffrant* et l'autre *déchiffrant*, comme le montre le tableau ci-dessous :

| Alphabet chiffrant | | Alphabet déchiffrant | |
|---|---|---|---|
| + = 321 | N = 223 | 111 = K | 223 = N |
| A = 213 | O = 123 | 112 = G | 231 = U |
| B = 232 | P = 113 | 113 = P | 232 = B |
| C = 122 | Q = 212 | 121 = V | 233 = S |
| D = 211 | R = 322 | 122 = C | 311 = L |
| E = 312 | S = 233 | 123 = O | 312 = E |
| F = 331 | T = 133 | 131 = M | 313 = H |
| G = 112 | U = 231 | 132 = I | 321 = + |
| H = 313 | V = 121 | 133 = T | 322 = R |
| I = 132 | X = 332 | 211 = D | 323 = Y |
| J = 333 | Y = 323 | 212 = Q | 331 = F |
| K = 111 | Z = 221 | 213 = A | 332 = X |
| L = 311 | W = 222 | 221 = Z | 333 = J |
| M = 131 | | 222 = W | |

Cet alphabet s'emploie comme le précédent et n'exige pas beaucoup plus de travail, bien que chaque lettre soit représentée par *trois* chiffres, au lieu de *deux*.

Pour chiffrer la phrase suivante :

*Il faut, autant qu'on peut, obliger tout le monde.*

En groupant par *sept*, on opérera ainsi (1) :

| | | |
|---|---|---|
| i l + f a u t | + + a u t a n | t + q u + o n |
| 1 3 3.3 2 2.1 | 3 3 2.2 1 2.2 | 1 3 2.2 3 1.2 |
| 3 1.2 3 1.3 3 | 2 2.1 3 3.1 2 | 3 2.1 3 2.2 2 |
| 2.1 1 1.3 1 3. | 1. 1 3 1.3 3 3. | 3.1 2 1.1 3 3. |
| TRMUXKH | XQWTVMJ | IUBINVT |
| + p e u t + + | o b l i g e r | + t o u t + l |
| 3 1 3.2 1 3.3 | 1 2 3.1 1 3.3 | 3 1 1.2 1 3.3 |
| 2 1.1 3 3.2 2 | 2 3.1 3 1.1 2 | 2 3.2 3 3.2 1 |
| 1.3 2 1.3 1 1. | 3.2 1 2.2 2 2. | 1.3 3 1.3 1 1. |
| HA+TZ+L | OPYMOQW | LAYSDFL |
| | e + m o n d e | + + + |
| | 3 3 1.1 2 2.3 | 3 3 3. |
| | 1 2.3 2 2.1 1 | 2 2 2. |
| | 2.1 1 3.3 1 2. | 1 1 1. |
| | FCERGPE | JWK |

ce qui donne, pour chiffre :

TRMUXKHXQWTVMJIUBINVTHA+TZ+L
OPYMOQWLAYSDFLFCERGPEJWK.

On voit clairement que chaque lettre du texte est représentée par trois chiffres, qui entrent chacun dans une combinaison différente pour former les nouvelles lettres constituant le cryptogramme.

Ainsi *i* fournit le premier chiffre de T, le second de M, et le troisième de X ; *l* fournit le second chiffre de T, le troisième de M, et le premier de K... La relation entre les lettres du texte et celles du cryptogramme sera rendue plus évidente, par

(1) Les doubles + indiquent les virgules ; la triple + représente le point final.

la notation déjà employée, ce qui fournit le tableau suivant :

| Texte. | Cryptogramme. |
|---|---|
| $i = T_1\ M_2\ X_3$ | $T = i_1\ l_1\ +_1$ |
| $l = T_2\ M_3\ K_1$ | $R = f_1\ a_1\ u_1$ |
| $+ = T_3\ U_1\ K_2$ | $M = t_1\ i_2\ l_2$ |
| $f = R_1\ U_2\ K_3$ | $U = +_2\ f_2\ a_2$ |
| $a = R_2\ U_3\ H_1$ | $X = u_1\ t_2\ i_3$ |
| $u = R_3\ X_1\ H_2$ | $K = l_3\ +_3\ f_3$ |
| $t = M_1\ X_2\ H_3$ | $H = a_3\ u_3\ t_3$ |

Les autres groupes de *sept* lettres reproduisent la même série de combinaisons. Inutile d'ajouter que cette série serait entièrement modifiée, si l'on choisissait tout autre nombre que *sept* pour base des groupements.

Toute lettre du chiffre est donc formée par la réunion, dans un ordre déterminé, de fragments provenant de trois lettres différentes et diversement situées dans le texte. Or, comme, dans un cryptogramme intercepté, rien ne peut indiquer de quel alphabet et de quel groupement on a fait usage pour l'écrire, le déchiffrement entraînerait des difficultés que l'on peut qualifier d'insurmontables.

En effet, l'alphabet étant donné, une même lettre peut être formée par 19,683 combinaisons différentes.

Soit, par exemple, le nombre 213, qui représente ici la lettre A. Le chiffre 2 entre, soit à la première place, à la seconde ou à la troisième, dans la composition de 27 lettres ; les chiffres 1 et 3 concourent également chacun à la formation de

27 lettres. Par suite, A ou 213 peut provenir de l'une quelconque des combinaisons *trois à trois* que sont susceptibles de former ces divers fragments. Leur nombre s'élève donc à 27 × 27 × 27 = 19,683. Il en résulte que, à la rigueur, la lettre A = 213 peut se reproduire 19,683 fois, sans avoir jamais la même signification, bien qu'on fasse usage d'un alphabet unique. Car, en admettant pour un instant que A soit formé par la combinaison $B_1$ $T_1$ $V_2$, dans laquelle $B_1 = 2$, $T_1 = 1$ et $V_2 = 3$, on est bien forcé d'admettre que le nombre 213 = A sera reproduit par toute autre combinaison, dans laquelle $T_1$ et $V_2$ conserveront leurs places et leurs valeurs, mais où $B_1$ sera remplacé par un autre fragment de lettre représentant le même chiffre, tels que $+_2$, $A_1$, $B_2$, $C_2$, $C_3$, . . ., etc. Or, ces fragments sont au nombre de 27 ; nous avons donc 27 combinaisons terminées par $T_1$ $V_2$ et fournissant le nombre 213.

$T_1$, à son tour, peut être remplacé par l'un des 27 fragments ayant 1 pour valeur, comme $+_3$, $A_2$, $C_1$, $D_2$, $D_3$, . . . .

$V_2$ peut de même être éliminé par un fragment égal à 3 ; ces fragments, $A_3$, $B_2$, $E_1$, $F_1$, $F_2$, . . . . sont aussi au nombre de 27.

Il y a donc 27 quantités susceptibles de prendre la première place dans la combinaison considérée, 27 capables d'occuper la seconde et 27 de remplir la troisième ; le nombre total des permutations possibles est donc bien de $27^3$ = 19,683.

Malgré ce nombre considérable de valeurs, chaque lettre ressort, à la traduction, avec sa vraie valeur, sans qu'il puisse jamais y avoir ambiguïté ou tâtonnement. Le déchiffrement se fait,

pour ainsi dire, mécaniquement, de même, du reste, que le chiffrement.

Pour qu'on puisse en juger, je reproduis le travail complet nécessaire pour déchiffrer la phrase suivante :

E+CXWFDPHNERERLLVHQ+EFVSYJRE GVZLDO+ISSZELTENQKXQZJ+M+CTMBPX NBGUDGBXSQPMET+CSQTPIAJQHGAESXD FNXZEL.

L'alphabet employé est celui de la page 36 et le groupement est alternativement de *onze*, *cinq* et *huit*, ce qu'on peut écrire : G = 11, 5, 8.

| | | |
|---|---|---|
| . . . . . . . . . . . | . . . . . | . . . . . . . . |
| E+CXWFDPHNE | RERLL | VHQ+EFVS |
| 3 1 2 3 2 1 1 2 2 3 3 | 3 2 2 3 1 | 1 2 1 3 1 3 2 1 |
| 2 2 2 2 3 3 1 2 1 1 1 | 2 3 2 2 3 | 2 3 2 1 3 1 2 3 |
| 1 3 3 1 3 2 2 3 3 1 2 | 1 1 3 1 1 | 3 1 1 2 1 2 3 3 |
| +on+signale | +un+m | ouvement |
| . . . . . . . . . . . | . . . . . | . . . . . . . . |
| YJREGVZLDO+ | ISSZE | LTENQKXQ |
| 3 2 3 3 3 3 3 2 2 3 1 | 1 3 2 2 3 | 3 1 1 1 3 3 3 1 |
| 2 1 1 2 1 2 1 2 2 1 3 | 3 2 3 3 2 | 2 2 2 3 2 1 2 1 |
| 1 1 2 1 1 1 2 3 3 2 1 | 2 1 3 1 2 | 1 1 3 3 2 2 1 2 |
| +de+l+ennem | i+sur | +votre+g |
| . . . . . . . . . . . | . . . . . | . . . . . . . . |
| ZJ+M+CTMBPX | NBGUD | GBXSQPME |
| 2 2 1 3 3 3 3 2 1 1 3 | 2 2 3 2 3 | 1 1 2 2 3 2 3 3 |
| 1 3 2 1 1 2 2 1 3 3 1 | 2 1 1 2 2 | 2 2 3 3 2 1 2 1 |
| 3 1 2 3 2 1 1 3 3 3 2 | 3 1 2 1 1 | 1 3 1 3 1 3 1 2 |
| auche++atte | ndez+ | vous+a+e |

| | | |
|---|---|---|
| . . . . . . . . . . . . | . . . . . | . . . . . . . . |
| T+CSQTPIAJQ | HGAES | XDFNXZEL |
| 1 3 3 3 2 1 1 2 2 2 3 | 3 1 3 1 1 | 3 3 2 2 1 1 3 3 |
| 3 2 1 2 1 3 3 1 1 3 1 | 2 2 1 3 3 | 1 2 2 3 3 3 2 2 |
| 3 2 2 1 3 3 3 3 2 1 2 | 1 2 2 3 3 | 2 1 3 1 2 3 1 1 |
| t r e+a t t a q u e | +c e t t | e+n u i t++ |

Il est facile, à l'inspection de ce tableau, de reconnaître comment on a procédé. Cependant, pour plus de clarté, je vais rappeler la méthode, en ne l'appliquant toutefois, pour éviter des longueurs, qu'à l'avant-dernier groupe : HGAES, ce qui suffira amplement à faire connaître la marche suivie.

On cherche, dans l'alphabet *chiffrant*, la valeur numérique de chaque lettre. Ces valeurs sont :

H = 313 ; G = 112 ; A = 213 ; E = 312 ; S = 233.

On écrit ces nombres *horizontalement* à la suite l'un de l'autre ; on les sépare par tranches de *cinq* chiffres, le groupement actuel étant de *cinq ;* puis on reporte sous le premier groupe, le second d'abord et ensuite le troisième :

31311
22133
12233

Il ne reste plus qu'à chercher, dans l'alphabet *déchiffrant*, la lettre qui correspond à chaque tranche *verticale* lue de haut en bas. On trouve ainsi :

321 = + ; 122 = c ; 312 = e ; 133 = t ; 133 = t.

Il est beaucoup plus pratique d'écrire directe-

ment les chiffres dans l'ordre qu'ils doivent occuper et on y arrive facilement avec un peu d'attention.

*
* *

On voit que le procédé est très simple et on est forcé d'admettre qu'un soldat, familiarisé avec lui par un exercice assez prolongé, pourra, même en campagne, chiffrer ou déchiffrer correctement une dépêche, sans la moindre difficulté.

D'un autre côté, le groupement, par ses innombrables variations, fournit à lui seul une garantie complète d'inviolabilité.

Donnons-en quelques exemples.

En chiffrant le mot : MARSEILLE, avec le même alphabet et la même méthode que précédemment, il viendra :

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| M | A | R | S | E | I | L | L | E | + |
| 1 | 2 | 3. | 2 | 3 | 1. | 3 | 3 | 3. | 3 |
| 3 | 1. | 2 | 3 | 1. | 3 | 1 | 1. | 1 | 2 |
| 1. | 3 | 2 | 3. | 2 | 2 | 1. | 1 | 2 | 1 |
| O | U | J | F | U | L | V | Y | Z | V |

En écrivant, au contraire, les chiffres *horizontalement*, et les relevant *verticalement*, on trouvera :

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| M | A | R | S | E | I | L | L | E | + |
| 1 | 3 | 1 | 2 | 1 | 3 | 3 | 2 | 2 | 2 |
| 3 | 3 | 3 | 1 | 2 | 1 | 3 | 2 | 3 | 1 |
| 1 | 3 | 1 | 1 | 3 | 1 | 2 | 3 | 2 | 1 |
| M | J | M | D | O | L | X | N | B | D |

Au lieu de lire les chiffres de gauche à droite, nous aurions pu les lire de droite à gauche ; on pourrait, de même, commencer par la troisième ligne, au lieu de la première ; ou bien encore lire la première de gauche à droite, ou réciproquement, la seconde en sens inverse et la troisième dans le même sens que la première (*en boustrophédon*).

On pourrait aussi lire les chiffres en diagonales. Pour simplifier cette opération, il est bon de les écrire à *niveau variable*, comme ceci :

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| M | A | R | S | E | I | L | L | E |
| 1 | — | 3 | — | 3. | — | 3 | — | 3 |
| 3. | 2 | 2 | 2. | 1 | 1 | 1. | 3 | 1 |
| 1. | 1 | 2 | 3. | 2 | 3 | 1. | 1 | 2 |
| — | 3. | — | 3 | — | 2 | — | 1. | — |
| T | J | W | K | L | O | U | O | + |

Pour avoir les lettres du cryptogramme, on a relevé les trois premiers chiffres de la première ligne : 133 = T, puis les deux derniers et le premier de la seconde ligne : 333 = J, etc.

On peut les écrire en losanges :

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| M | A | R | S | E | I | L | L | E |
| 1 | — | — | 2 | — | — | 3. | — | — |
| 3 | 2 | — | 3. | 3 | — | 1 | 3. | — |
| 1 | 1 | 3. | 3 | 1 | 1. | 1 | 1 | 3. |
| — | 3 | 2 | — | 2. | 3 | — | 1 | 1. |
| — | — | 2 | — | — | 2 | — | — | 2. |
| O | Y | H | P | L· | P | R | L | W |

En lisant chaque losange à part, on aurait :

IPRSLBHPG ;

ou en triangles renversés :

| M | A | R | S | E | I | L | L | E |
|---|---|---|---|---|---|---|---|---|
| 1 | — | — | — | 3 | — | — | — | 3. |
| 3 | 2 | — | 2. | 1 | 1 | — | 3. | 1 |
| 1 | 1. | 3 | 3 | 2. | 3 | 3 | 1. | 2 |
| — | 3 | 2. | 3 | — | 2 | 1. | 1 | — |
| — | — | 2 | — | — | — | 1 | — | — |
| T | R | P | K | X | F | B | + | V |

On peut encore opérer la bipartition des groupes :

| M | A | R | S | E | I | L | L | E |
|---|---|---|---|---|---|---|---|---|
| 1 | — | 3 | — | 3. | — | 3 | — | 3 |
| 3. | — | 2 | — | 1 | — | 1. | — | 1 |
| 1 | — | 2. | — | 2 | — | 1 | — | 2 |
| — | 2 | — | 2 | — | 1. | — | 3 | — |
| — | 1 | — | 3. | — | 3 | — | 1 | — |
| — | 3. | — | 3 | — | 2 | — | 1. | — |
| T | J | D | G | Q | Z | H | H | + |

etc., etc., etc.

Je ne crois pas que ces derniers systèmes soient à recommander ; ils sont plus compliqués, mais ne semblent pas offrir beaucoup plus de garanties.

Le mode de groupement peut être indiqué dans le cryptogramme même, soit à l'aide de lettres convenues intercalées à un rang déterminé, soit à l'aide de chiffres *arabes* d'une valeur conventionnelle. Mais je n'insisterai pas à ce sujet, mon but étant de faire connaître un nouveau système et non de rédiger un manuel de cryptographie *militaire*.

Aussi bien que le groupement, l'alphabet est

variable et la base de sa confection peut être indiquée dans les dépêches chiffrées.

Un moyen très simple d'établir un alphabet à l'aide d'un petit nombre de chiffres, ou même d'un seul, repose sur le système de punition militaire employé par les Romains et, depuis, par divers généraux, notamment par l'archiduc Léopold en 1642, et par le maréchal de Créqui en 1675, actuellement encore, dit-on, pratiqué en Espagne.

Ce système, nommé *décimation*, consistait à ranger en cercle les soldats coupables de sédition ou de lâcheté et à mettre à mort ceux qui occupaient les dixième, vingtième, etc,, rangs, à partir de l'un d'eux désigné au hasard. Parfois la décimation se continuait jusqu'à l'extinction totale des coupables.

L'historien Josèphe rapporte que, pendant le siège de Jotaparte, ses soldats, découragés et surexcités par le désespoir, la famine et les souffrances qu'ils enduraient, résolurent de se décimer eux-mêmes jusqu'au dernier, celui-là devant se tuer lui-même plutôt que de se soumettre aux Romains. Josèphe, alors gouverneur de Galilée, et le seul soldat en qui il eût confiance, échappèrent seuls au massacre et se rendirent à Vespasien. L'historien autobiographe attribue ce résultat à la protection céleste, qui leur fit prendre, à lui la dernière place et à son compagnon l'avant-dernière. Néanmoins quelques commentateurs ont supposé que Josèphe avait simplement calculé le rang qu'il devait occuper pour survivre à ses compagnons et même celui qu'il avait fait prendre à son plus fidèle soldat.

Cette supposition n'a rien d'invraisemblable,

car le hasard, qui semble présider à une telle opération, n'est qu'apparent et ne peut tromper que des hommes grossiers ou manquant de réflexion. Un esprit attentif, au contraire, parvient sans peine à déterminer l'ordre dans lequel chaque *numéro sortira*, pour ainsi dire, cet ordre étant invariable quand les conditions sont les mêmes, c'est-à-dire le *total* des objets à décimer, le *nombre* par lequel on décime et enfin le point de départ.

Pour nous rapprocher du système de *décimation* employé par les anciens, prenons un paquet de cartes, sur chacune desquelles nous inscrirons une des lettres de l'alphabet. Le nombre de ces cartes sera de 25 pour l'alphabet à *deux chiffres* et de 27 pour celui à *trois chiffres*. Le travail étant le même dans les deux cas, nous ne nous occuperons que du dernier.

Les lettres étant rangées dans l'ordre alphabétique, en commençant par + et finissant par W, nous mettrons dessous, une à une, la première, la seconde, la troisième,... en comptant; nous prélevons la dixième et recommençons à compter de 1 à 10, en faisant passer, l'une après l'autre, chaque carte de dessus dessous, en prélevant toujours la dixième. En continuant jusqu'au bout, nous aurons classé les lettres dans l'ordre suivant :

I, S, B, M, Y, H, U, F, T, G, X, L, A, R, N, E, C, +, D, K, Q, J, W, P, V, O, Z,

pour l'alphabet de 27 lettres, et dans le suivant :

J, T, E, P, B, N, A, O, D, S, I, Z, U, M, K, H, L, R, Y, Q, G, X, C, V, F,

pour l'alphabet de 25 lettres.

Il ne reste plus, pour avoir la valeur numérique de nos lettres, qu'à attribuer à la première le nombre 111 ou 11, suivant le cas ; à la seconde, 112 ou 12 ; à la troisième, 113 ou 13 ; à la suivante, 121 ou 14, etc., les nombres se suivant dans l'ordre numérique.

L'emploi des cartes est loin d'être indispensable ; il semble même plus pratique et, à coup sûr, plus prompt, d'écrire les lettres, d'une part, et les combinaisons de chiffres d'autre part, dans leur ordre naturel, puis de décimer, en inscrivant immédiatement sa valeur, auprès de chaque terme de ces deux séries.

Le point de départ de la décimation étant arbitraire, ainsi que le nombre par lequel on décime, nous décimerons, dans l'exemple suivant, par le nombre 4, en commençant à K.

| | | | |
|---|---|---|---|
| + = 211 | N = 111 | 111 = N | 223 = D |
| A = 321 | O = 323 | 112 = R | 231 = L |
| B = 233 | P = 132 | 113 = V | 232 = T |
| C = 122 | Q = 221 | 121 = W | 233 = B |
| D = 223 | R = 112 | 122 = C | 311 = M |
| E = 212 | S = 322 | 123 = G | 312 = Z |
| F = 333 | T = 232 | 131 = K | 313 = I |
| G = 123 | U = 133 | 132 = P | 321 = A |
| H = 332 | V = 113 | 133 = U | 322 = S |
| I = 313 | X = 331 | 211 = + | 323 = O |
| J = 213 | Y = 222 | 212 = E | 331 = X |
| K = 131 | Z = 312 | 213 = J | 332 = H |
| L = 231 | W = 121 | 221 = Q | 333 = F |
| M = 311 | | 222 = Y | |

Ayant préparé la série alphabétique et la série

numérique, K étant le point de départ et 4 la base de décimation, j'ai compté 1 sur K, 2 sur L, 3 sur M et 4 sur N ; auprès de N, j'ai inscrit le premier groupe de chiffres, 111. Réciproquement, j'ai posé N auprès de 111.

Comptant ensuite 1 sur O, 2 sur P, 3 sur Q et 4 sur R, cette lettre a reçu 112 pour valeur et auprès de 112 j'ai inscrit R.

J'ai trouvé, de même, V = 113, W = 121, C = 122, G = 123, K = 131. Continuant de compter 1 sur L, 2 sur M, j'ai dû, sans m'occuper de N qui est censé avoir été enlevé, compter 3 sur O et 4 sur P ; P a donc reçu 132 pour chiffre. On voit la marche de l'opération.

Je dois faire observer qu'au lieu de décimer la série littérale, on peut décimer la série numérique ; le résultat n'étant pas le même dans les deux cas, il importe que les conventions entre correspondants soient précises et suffisamment détaillées pour éviter toute erreur. Ces conventions peuvent, du reste, porter non seulement sur les points déjà signalés, mais encore sur une foule d'autres. Par exemple, au lieu de l'ordre naturel des lettres et des chiffres, on peut admettre, pour base des alphabets, un ordre conventionnel quelconque.

Appliquons l'alphabet que nous venons d'établir à une phrase et rapprochons les lettres du cryptogramme de celles de sa traduction pour voir l'influence des répétitions de lettres et même de mots d'une certaine longueur.

Ici, on a groupé par 23 et l'alphabet a été obtenu en décimant par 4, en commençant à compter sur K ; toutes conditions qui peuvent s'écrire : D = 4 : K ; G = 23.

l a+c r y p t o g r a p h i e+a n c i e n n e+o p é r
TRGVUDVJEGSGMW+NCYHCARACZUDRDY

a i t+s u r +l e s+l e t t r e s+e n t i è r e s
QRMJGVWIZPQATR+YGQTGDGSWWVNW

+t a n d i s+q u e+ l a+c r y p t o g r a p h i e+
AEGCEGYEVAPD+EMISKWAEHEXNLNRY

n o u v e l l e+n+o p è r e+q u e +s u r+ d e s+f
BETVHYEZCELCBMRMRMLW++PYVEASLZ

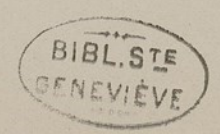
r a c t i o n s+ d e+ l e t t r e s++
XSYYGQZLEWKXWVEBWACY+.

On voit que les répétitions de lettres, dans le texte, n'entraînent pas de répétitions analogues dans le chiffre, malgré la longueur des assemblages de lettres répétées, puisque les mots : *la+cryptographie* +, +*oper*, + *sur* +, + *lettres* +, sont reproduits deux fois dans la phrase et que le chiffre ne présente rien de semblable.

Il faut, en effet, pour qu'une réunion de lettres soit représentée deux fois par les mêmes signes, que cette réunion figure dans deux groupements semblables et qu'elle occupe la même place dans chacun, ce qu'on peut toujours éviter par l'addition ou la suppression du signe +.

Exemple : PARIS ++ et + PARIS + nous fourniront deux chiffres différents, bien que le groupement soit le même :

| | |
|---|---|
| PARIS++ | +PARIS+ |
| 1313322 | 2131332 |
| 3211211 | 1321121 |
| 2123211 | 1212321 |
| KHTRRG+ | JUJ++EA |



On a donc : PARIS + + = KHTRRG + et + PARIS + = JUJ + + EA ; cependant alphabet et groupement sont identiques.

Nous avons vu qu'il est impossible d'employer un alphabet comportant plus de *trois* chiffres à chaque combinaison. Il ne faudrait pourtant pas en conclure qu'il est impossible de scinder les lettres en plus de trois fragments. En faisant usage, à la fois, de deux alphabets *différents* ou non, on obtient la fragmentation des lettres en quatre, six ou neuf parties. On peut même aller beaucoup plus loin, mais il faut alors augmenter le nombre des alphabets. Trois alphabets fourniraient la fragmentation de chaque lettre en 8, 12, 18 ou 27 parties, selon que l'on se servirait exclusivement d'alphabets à 2 chiffres, ou d'abord d'alphabets à 2 chiffres puis d'alphabets à 3, ou exclusivement d'alphabets à 3 chiffres.

Avec *quatre* alphabets, on pourrait fractionner chaque lettre en 16, 24, 36, 54 et même 81 parties, mais le chiffrage serait laborieux et la traduction pénible.

Je ne parle donc de ces méthodes que pour mémoire et me contente d'exposer le mode de division des lettres en *six* parties, ce système, assez simple, pouvant rendre des services dans certains cas et montrant, en outre, quelles ressources présente la cryptographie nouvelle.

Il est nécessaire, pour effectuer ce travail, d'établir deux alphabets, l'un à deux chiffres, l'autre à trois, tous les deux *chiffrant* et *déchiffrant*. L'arrangement le plus commode et le plus pratique est le suivant, où la colonne du milieu de chaque

série est dans l'ordre naturel, les autres donnant le résultat du décimage.

| | | |
|---|---|---|
| 121...+... » | | 58...111...F |
| 333...A...75 | G...44...232 | 87 ..112...M |
| 223...B...55 | N...45 ..311 | 68...113...T |
| 221...C...47 | U...46...331 | »...121...+ |
| 323...D...65 | C...47...221 | 86...122...H |
| 132...E...67 | K...48...312 | 66...123...P |
| 111...F...58 | S...54...213 | 76...131...Y |
| 232...G...44 | B...55...223 | 67...132...E |
| 122...H...86 | L...56...321 | 88 ..133. .O |
| 212...I...84 | V...57...322 | 78...211...Z |
| 313...J...74 | F...58...111 | 84...212...I |
| 312...K...48 | Q...64...222 | 54...213...S |
| 321...L...56 | D...65...323 | 47...221...C |
| 112...M...87 | P...66...123 | 64...222...Q |
| 311...N...45 | E...67...132 | 55...223...B |
| 133...O...88 | T...68...113 | 85...231...R |
| 123...P...63 | J ...74...313 | 44...232...G |
| 222...Q...64 | A...75...333 | 77...233...X |
| 231...R...85 | Y...76...131 | 45...311...N |
| 213...S...54 | X...77...233 | 48...312...K |
| 113...T...68 | Z...78...211 | 74...313...J |
| 331...U...46 | I....84. .212 | 56...321...L |
| 322...V...57 | R...85..231 | 57...322...V |
| 233...X...77 | H...86...122 | 65...323...D |
| 131...Y...76 | M...87...112 | 46...331...U |
| 211...Z.. 78 | O ..88...133 | »...332..W |
| 332 ..W.. » | | 75...333...A |

On remarquera que, pour mieux éviter les chances d'erreurs, on a fait usage, dans les combinaisons numériques de l'alphabet à 25 lettres, des chiffres 4, 5, 6, 7 et 8, à l'exclusion de 1, 2 et

3 qui sont employés par l'alphabet de 27 lettres.

Les deux alphabets ont été décimés par *sept*.

Traduisons le passage suivant :

Autrefois le rat de ville
Invita le rat des champs,
D'une façon fort civile,
A des reliefs d'ortolans.

L'un des alphabets étant dépourvu du signe +, nous ne séparerons pas les mots.

Groupons par *sept* et étudions l'opération sur le premier groupe : *Autrefo*.

Les lettres de ce groupe ont pour valeurs, dans l'alphabet à deux chiffres :

A = 75 ; u = 46 ; t = 68 ; r = 85 ; e = 67 ; f = 58 ; o = 88 ; ce qui donne :

| | | | | | | |
|---|---|---|---|---|---|---|
| A | u | t | r | e | f | o |
| 7 | 4 | 6 | 8 | 6 | 5 | 8 |
| 5 | 6 | 8 | 5 | 7 | 8 | 8 |

Relevant les chiffres deux à deux et *horizontalement*, il viendra : 74 = J ; 68 = T ; 65 = D ; 85 = R ; 68 = T ; 57 = V ; 88 = O, ou JTDRTVO, assemblage de lettres auquel nous appliquerons l'alphabet à *trois* chiffres, ce qui fournira le cryptogramme cherché.

Pour abréger, au lieu de chercher les lettres qui forment la première traduction, on remplace immédiatement chaque groupe de *deux* chiffres par le groupe de *trois* chiffres correspondant ; c'est-à-dire, au lieu de chercher la valeur de 74 = J, puis celle de J = 313, on lit directement, dans le deuxième tableau : 74 = 313, et ainsi des autres.

| | | |
|---|---|---|
| autreto | islerat | deville |
| 7468658 | 8556876 | 6658556 |
| 5685788 | 4467558 | 5774667 |
| 3132131 | 2312331 | 1123231 |
| 1123123 | 3212331 | 2122333 |
| 3331323 | 1122131 | 3133312 |
| JSFRXUD | RXEPNHY | MD+BAOK |

| | | |
|---|---|---|
| invital | eratdes | champsd |
| 8458675 | 6876665 | 4878656 |
| 4574856 | 7558574 | 7657645 |
| 2112333 | 1113223 | 3231313 |
| 1131212 | 1322231 | 1123231 |
| 2123221 | 3132313 | 2132311 |
| ZXNKHPC | FVJQJEJ | DYNGKEN |

| | | |
|---|---|---|
| unefaco | nfortci | vileade |
| 4465748 | 4588648 | 5856766 |
| 6578578 | 5885874 | 7467557 |
| 2331322 | 3122113 | 1311333 |
| 3212231 | 1323311 | 1233332 |
| 2332211 | 1321313 | 1112132 |
| XEGHKWZ | KZJXFLJ | YOKALME |

| | | |
|---|---|---|
| srelief | sdortol | ans |
| 5865865 | 5688685 | 745 |
| 4576478 | 4585886 | 554 |
| 1312322 | 3112111 | 322 |
| 1221221 | 2311112 | 121 |
| 1323221 | 1333112 | 333 |
| YGIIZDC | NZPF+AM | V+A |

Comme dans le chiffrage à une clé simple, le groupement peut être varié à volonté *pour chaque clé*.

La traduction s'obtient par l'opération inverse de celle qui a servi à chiffrer.

Soit à traduire :

REZH+XMDYS+LFBNNZGTBE,

sachant que cette phrase, chiffrée à l'aide du tableau précédent, a été groupée par *trois* pour l'alphabet à *deux* chiffres, et par *cinq* pour l'alphabet à *trois* chiffres.

D'après la méthode que nous employons, il faut, pour la traduction, écrire les nombres *horizontalement* et les relever *verticalement*. Voici l'opération :

| | | | | |
|---|---|---|---|---|
| . . . . . | . . . . . | . . . . . | . . . . . | . |
| REZH+ | XMDYS | +LFBN | NZGTB | E |
| 2 3 1 1 3 | 2 3 3 1 1 | 1 2 1 3 2 | 3 1 1 2 1 | 1 |
| 2 2 1 1 1 | 2 3 2 3 1 | 1 1 1 1 2 | 1 2 3 2 1 | 3 |
| 2 2 1 2 1 | 3 1 2 1 3 | 2 3 3 1 1 | 1 3 2 2 3 | 2 |
| . . . . . | . . . . . | . . . . . | . . . . . | . |

| | | | | | | |
|---|---|---|---|---|---|---|
| 6 4 5 | 8 7 4 | 4 6 5 | 6 8 8 | 6 8 4 | 4 5 6 | 6 4 6 |
| 7 5 8 | 5 5 5 | 7 7 6 | 7 5 4 | 5 4 7 | 6 6 7 | 8 6 7 |
| e n f | r a n | c e l | e r i | d i c | u l e | t u e |

Ceux qui seraient curieux de savoir comment se groupent les fragments de lettres divisées en *six* parties, pourront en juger par le relevé ci-après des quinze premières lettres des deux cryptogrammes qui précèdent :

| | |
|---|---|
| $J = a_1\ u_1\ t_1\ r_1\ e_1\ f_1$ | $R = e_1\ n_1\ f_1\ e_4\ n_1\ f_4$ |
| $S = o_1\ a_4\ u_4\ t_4\ r_4\ e_4$ | $E = r_1\ a_1\ n_1\ r_4\ e_2\ n_2$ |
| $F = f_4\ o_4\ a_2\ u_2\ t_2\ r_2$ | $Z = f_2\ e_5\ n_5\ f_5\ r_2\ a_2$ |
| $R = e_2\ f_2\ o_2\ a_5\ u_5\ t_5$ | $H = n_2\ r_5\ e_3\ n_3\ f_3\ e_6$ |
| $X = r_5\ e_5\ f_5\ o_5\ a_3\ u_3$ | $+ = n_6\ f_6\ r_3\ a_3\ n_3\ r_6$ |
| $U = t_3\ r_3\ e_3\ f_3\ o_3\ a_6$ | $X = a_4\ n_4\ c_1\ e_1\ l_1\ c_4$ |
| $D = u_6\ t_6\ r_6\ e_6\ f_6\ o_6$ | $M = e_4\ l_4\ e_1\ r_1\ a_5\ n_5$ |
| $R = i_1\ s_1\ l_1\ e_1\ r_1\ a_1$ | $D = c_2\ e_2\ l_2\ c_5\ e_5\ l_5$ |
| $X = t_1\ i_4\ s_4\ l_4\ e_4\ r_4$ | $Y = e_2\ r_2\ a_6\ n_6\ c_3\ e_3$ |
| $E = a_4\ t_4\ i_2\ s_2\ l_2\ e_2$ | $S = l_3\ c_6\ e_6\ l_6\ e_3\ r_3$ |
| $P = r_2\ a_2\ t_2\ i_5\ s_5\ l_5$ | $+ = i_1\ e_4\ r_4\ i_4\ d_1\ i_1$ |
| $N = e_5\ r_5\ a_5\ t_5\ i_3\ s_3$ | $L = c_1\ d_4\ i_4\ c_4\ i_2\ e_5$ |
| $H = l_3\ e_3\ r_3\ a_3\ t_3\ i_6$ | $F = r_5\ i_5\ d_2\ i_2\ c_2\ d_5$ |
| $Y = s_6\ l_6\ e_6\ r_6\ a_6\ t_6$ | $B = i_5\ c_5\ i_3\ e_6\ r_6\ i_6$ |
| $M = d_1\ e_1\ v_1\ i_1\ l_1\ l_1$ | $N = d_3\ i_3\ c_3\ d_6\ i_6\ c_6$ |

Les indices qui accompagnent chaque lettre indiquent l'ordre des *sixièmes* de cette lettre.

Maintenant, combien de valeurs différentes possèdent les lettres d'un cryptogramme de ce genre ?

Nous avons vu qu'avec un alphabet à *deux* chiffres, chaque lettre a 100 valeurs ; qu'avec un alphabet à *trois* chiffres, elle en possède 19,683. Les deux alphabets employés conjointement permettront donc de représenter chaque lettre de $100 \times 19{,}693 = 1{,}968{,}300$ manières diverses. Dans ce calcul, il n'est pas tenu compte de la dispersion des fragments de lettres, dispersion qui augmente considérablement la difficulté du déchiffrement sans clé, au point de le rendre, si je ne me trompe, complètement impossible.

On est cependant conduit à se demander si les

*sixièmes* de lettres existent réellement, car, quoi qu'on fasse, il est impossible de les isoler.

Ces *sixièmes*, de même que les *quarts*, les *neuvièmes*, etc., peuvent être comparés aux quantités algébriques dites *imaginaires*, qui n'ont aucune valeur réelle, mais dont les produits sont réels.

Il est, du reste, facile de s'en assurer. Examinons le cas le plus simple, celui où on se sert d'un alphabet à *deux* chiffres, en donnant toutefois *deux tours de clé*.

Prenons par exemple le mot: FEMME, que nous chiffrons, suivant les conventions habituelles, à l'aide de l'alphabet décimé par *sept*. Il vient :

*FEMME*
5 6 8 8 6
8 7 7 7 7

Maintenant nous relevons horizontalement les nombres : 56, 88, 68, 77 et 77, mais, au lieu de les traduire en lettres, nous les écrivons en colonnes verticales :

5 8 6 7 7
6 8 8 7 7

Relevant, de nouveau horizontalement, ces chiffres, *deux à deux*, nous les remplaçons par des lettres et avons pour cryptogramme :

FEYOX.

En fonction des lettres du texte, les dernières ont les valeurs suivantes :

$$\mathrm{F_1\,F_2} = F_1\,M_1\,;\ \mathrm{E_1\,E_2} = E_1\,E_2\,;\ \mathrm{Y_1\,Y_2} = M_2\,E_1\,;$$
$$\mathrm{O_1\,O_2} = M_1\,F_2\,;\ \mathrm{X_1\,X_2} = M_2\,E_2.$$

Mais ce résultat est un cas particulier résultant de l'emploi d'un seul alphabet pour les deux chiffrages. Dans ce cas, évidemment, les chiffres affectés à la représentation des lettres n'éprouvent aucun changement de nombre ou de valeur ; leur assemblage seul est modifié. Il n'en est plus ainsi dans le cas général, car, alors, le premier chiffrage ayant eu pour résultat de condenser, en une seule lettre, deux chiffres provenant de lettres différentes, le second, en opérant de même sur les lettres ainsi obtenues, la lettre finale est bien la résultante de quatre lettres distinctes groupées d'une certaine façon.

Ainsi F est formé : 1° du premier chiffre fourni par le groupement des premiers chiffres de F et de E ; 2° du premier chiffre fourni par le groupement des premiers chiffres de M et de $M_1$ ce qu'on peut écrire :

$$F = (F_1\ E_1)_1\ (M_1\ M_1)_1 \quad \text{ou} \quad F_1\ E_1\ M_1\ M_1$$
$$E = (E_1\ F_2)_1\ (E_2\ M_2)_1 \qquad E_1\ F_3\ E_3\ M_3$$
$$Y = (M_2\ E_2)_1\ (F_1\ E_1)_2 \qquad M_3\ E_3\ F_2\ E_2$$
$$O = (M_1\ M_1)_2\ (E_1\ F_2)_2 \qquad M_2\ M_2\ E_2\ F_4$$
$$X = (E_2\ M_2)_2\ (M_2\ E_2)_2 \qquad E_4\ M_4\ M_4\ E_4$$

les dernières valeurs étant obtenues en faisant $(F_1)_1 = F_1$ ; $(F_1)_2 = F_2$ ; $(F_2)_1 = F_3$ ; $(F_2)_2 = F_4$, ce qui simplifie les formules et les rend plus claires et plus faciles à comparer.

Chiffré de la même manière et avec le même alphabet, le mot LUNDI se traduira : SHSPS et on aura :

$$
\begin{aligned}
S &= (L_1\, U_1)_1\, (N_1\, D_1)_1 = L_1\, U_1\, N_1\, D_1 \\
H &= (I_1\, L_2)_1\, (U_2\, N_2)_1 = I_1\, L_3\, U_3\, N_3 \\
S &= (D_2\, I_2)_1\, (L_1\, U_1)_2 = D_3\, I_3\, L_2\, U_2 \\
P &= (N_1\, D_1)_2\, (I_1\, L_2)_2 = N_2\, D_2\, I_2\, L_4 \\
S &= (U_2\, N_2)_2\, (D_2\, I_2)_2 = U_4\, N_4\, D_4\, I_4
\end{aligned}
$$

Il convient d'examiner si une clé simple à deux ou à trois chiffres est susceptible de fournir les résultats donnés par l'emploi de deux clés ou par le double emploi d'une clé unique.

De FEMME = FEYOX, on déduit :

$$
\begin{array}{lll}
F_1 = F_1 & E_1 = Y_1 & M_2 = X_1 \\
E_1 = F_2 & F_2 = Y_2 & E_2 = X_2 \\
M_1 = E_1 & E_2 = O_1 & \\
M_1 = E_2 & M_2 = O_2 &
\end{array}
$$

d'où, en rapprochant les quantités semblables :

$$
E_1 = E_2 = Y_1 = Y_2 = F_2 = M_1 = O_1 = X_2,
$$
$$
F_1 = F_1\,;\;\; M_2 = O_2 = X_1.
$$

Il en résulte qu'aucun alphabet de deux chiffres ne peut, dans les conditions employées, donner directement FEMME = FEYOX, car il faudrait avoir E = Y et M = O, ce qui est impossible.

Un alphabet à trois chiffres, exigeant E = O, cette combinaison est également impossible.

Les combinaisons de *quatre* chiffres, ne pouvant s'appliquer qu'à des alphabets de $2^4 = 16$ lettres ou de $3^4 = 81$ lettres, doivent aussi être rejetées.

On ne peut donc remplacer ce système par un autre plus simple.

Il arrive cependant que certains groupes de lettres pourraient être traduits par un alphabet unique. Ainsi le mot LUNDI = SHSPS ne peut être obtenu à l'aide d'un alphabet à deux chiffres, car il faudrait faire S = L ; mais rien n'empêche d'obtenir ce résultat avec un alphabet à *trois* chiffres.

Soit encore le mot FRANCE, que nous chiffrerons avec un alphabet où A = 41, C = 52, E = 31, F = 13, I = 34, N = 23, R = 14, S = 12 et U = 53.

Il viendra :

FRANCE
1 1 4 2 5 3
3 4 1 3 2 1

1 4 5 3 1 2
1 2 3 4 3 1
RUSSIE

Aucun alphabet à deux chiffres ne pourra fournir directement FRANCE = RUSSIE, tandis que ce résultat sera facilement obtenu avec un alphabet à trois chiffres.

Faisons, par exemple, A = 322, C = 112, E = 123, F = 131, I = 132, N = 231, R = 113, S = 312 et U = 211, nous aurons :

FRANCE
1 1 3 2 1 1
3 1 2 3 1 2
1 3 2 1 2 3
RUSSIE

Lorsqu'on opère le chiffrage en employant successivement deux alphabets à *trois* chiffres, ou deux fois de suite le même alphabet, on scinde

chaque lettre en *neuvièmes* et les lettres du cryptogramme prennent les valeurs suivantes :

En groupant par *dix*,

| | | |
|---|---|---|
| 1^re^ lettre | = | $A_1$ $B_1$ $C_1$ $D_1$ $E_1$ $F_1$ $G_1$ $H_1$ $I_1$ |
| 2^e^ — | = | $J_1$ $A_4$ $B_4$ $C_4$ $D_4$ $E_4$ $F_4$ $G_4$ $H_4$ |
| 3^e^ — | = | $I_4$ $J_4$ $A_7$ $B_7$ $C_7$ $D_7$ $E_7$ $F_7$ $G_7$ |
| 4^e^ — | = | $H_7$ $I_7$ $J_7$ $A_2$ $B_2$ $C_2$ $D_2$ $E_2$ $F_2$ |
| 5^e^ — | = | $G_2$ $H_2$ $I_2$ $J_2$ $A_5$ $B_5$ $C_5$ $D_5$ $E_5$ |
| 6^e^ — | = | $F_5$ $G_5$ $H_5$ $I_5$ $J_5$ $A_8$ $B_8$ $C_8$ $D_8$ |
| 7^e^ — | = | $E_8$ $F_8$ $G_8$ $H_8$ $I_8$ $J_8$ $A_3$ $B_3$ $C_3$ |
| 8^e^ — | = | $D_3$ $E_3$ $F_3$ $G_3$ $H_3$ $I_3$ $J_3$ $A_6$ $B_6$ |
| 9^e^ — | = | $C_6$ $D_6$ $E_6$ $F_6$ $G_6$ $H_6$ $I_6$ $J_6$ $A_9$ |
| 10^e^ — | = | $B_9$ $C_9$ $D_9$ $E_9$ $F_9$ $G_9$ $H_9$ $I_9$ $J_9$ |

et en groupant par *cinq*,

| | | |
|---|---|---|
| 1^re^ lettre | = | $A_1$ $B_1$ $C_1$ $D_1$ $E_1$ $A_4$ $B_4$ $C_4$ $D_4$ |
| 2^e^ — | = | $E_4$ $A_7$ $B_7$ $C_7$ $D_7$ $E_7$ $A_2$ $B_2$ $C_2$ |
| 3^e^ — | = | $D_2$ $E_2$ $A_5$ $B_5$ $C_5$ $D_5$ $E_5$ $A_8$ $B_8$ |
| 4^e^ — | = | $C_8$ $D_8$ $E_8$ $A_3$ $B_3$ $C_3$ $D_3$ $E_3$ $A_6$ |
| 5^e^ — | = | $B_6$ $C_6$ $D_6$ $E_6$ $A_9$ $B_9$ $C_9$ $D_9$ $E_9$ |

Ce qui précède suffit pour guider les chercheurs curieux d'aller plus loin et d'étudier des fragments de lettres encore plus petits.

*
* *

M. Kerckhoffs a énuméré ainsi (*Cryptographie militaire*, page 8) les qualités que doit posséder un système de cryptographie militaire :

1° Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;

2° Il faut qu'il n'exige pas de secret et qu'il

puisse sans inconvénient tomber entre les mains de l'ennemi ;

3° La clé doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;

4° Il faut qu'il soit applicable à la correspondance télégraphique ;

5° Il faut qu'il soit portatif et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;

6° Il doit être d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

Et, après avoir examiné tous les systèmes connus, M. Kerckhoffs conclut que la solution du problème doit être cherchée dans l'application de quelque appareil mécanique, basé sur le principe d'interversion, c'est-à-dire dans l'emploi d'un cryptographe.

M. le commandant Josse, après avoir reproduit les six conditions posées par le savant professeur, en tirait des conclusions diamétralement opposées :

7° « Il faut que le système ne comporte pas » l'emploi d'un livre ou d'un appareil ».

Et il ajoute :

« La cryptographie militaire, proprement dite, » doit employer un système n'exigeant qu'un » crayon et du papier. » (*La Cryptographie*, p. 99.

En effet, en temps de guerre, il est toujours à craindre ou que l'appareil, *en état de fonctionner*, tombe entre les mains de l'ennemi, ou que l'officier qui reçoit un cryptogramme se trouve, par fortune de guerre, démuni de l'appareil qui seul peut lui permettre de lire la dépêche reçue.

Non seulement le système que je viens d'exposer satisfait aux sept conditions ci-dessus, mais il permet d'en ajouter une nouvelle, dont l'importance n'échappera à personne :

*Le rapprochement d'un cryptogramme et de sa traduction ne doit jamais permettre de découvrir la clé et, par suite, de déchiffrer la partie non traduite d'une dépêche dont on possède le reste en clair.*

Ce qui s'obtient facilement et sûrement en donnant deux tours de clé.

⁂

EXERCICES

Traduire, sachant qu'on a fait usage d'un alphabet à *trois* chiffres décimé par 7 et qu'on a groupé par 5, 4, 7, soit : D = 7, + 1 et G = 5, 4, 7.

CQUNLFEEONKYBRJSUSXMSMPFXOFBE UM+SSAIF+PJYOFRGBEFMMNIU+DJ+LYPV B+MHSNUSNMROLKOB+FRIKUAMSKXYFU +KLRLMZ.

Alphabet de la page 28, G = 8 ;

UE+BWMHHNSTEQSDWPNJYROMDFPEO EPLAJVIPXWYXCJHCZD.

Alphabet à *deux* chiffres.
D = 2, 5 ; Q = 1 — G = 5, 4 ou : décimez par 2

et 5 en commençant à Q ; groupez par 5 et 4, alternativement.

YBAOLLAEZHPYURBXIULCUPOXKPSYEG HKGDPQHREE.

Alphabet à *deux* chiffres. — Décimez les *nombres* par 3, au départ de 31. Groupez par 11.

FUOVVRYQIKFDOZHVAJEDORNRFUMTVI JM.

Même alphabet. — Deux tours de clé : le premier en groupant par 5 ; le second en groupant par 5 également.

QOSGJENDSDQSEKPXFVREOGKANVRRXI KNNIXPNHODORRPKDPSO.

(Les groupements indiqués se rapportant à l'*écriture*, il convient d'en intervertir l'ordre pour la *lecture*.)

Alphabet à *trois* chiffres : décimez par 4, au départ de P. — Deux tours de clé : le premier en groupant alternativement par 2 et 5 ; le second, en groupant uniformément par 4.

MQWJ+TDYXWSWMDSOSH+RFEVASOX WSDCDSNRJUHPFDPPN.

Même alphabet, même groupement, même phrase que dessus, pour montrer le changement qu'entraine le déplacement d'un point.

WWV+OCMRVFORR+BPWSUSLUDHDRF RHOSPXSPAOOJOSXW+.

Alphabet à *trois* chiffres : décimez les *nombres* par 4, au départ de 121. — Deux tours de clé : le premier, en groupant par 8 ; le second en groupant par 10.

JI+GEZCIENAEZGQDMEENKJPEKENU+G
JEXOYZWWECRSWYTKNJJK+I+CQKX+.

* * *

Aux cryptologues qui croient qu'il est toujours possible d'achever la traduction d'un cryptogramme à demi-déchiffré, j'offre le problème suivant :

Connaissant la traduction de la première phrase du chiffre ci-après, lire la seconde, sachant que le chiffrage est exactement le même dans les deux.

FKKAJTMD+OP+LUDEW+CJJWXUFYXN
KJX+C++JOWTQHTTJ+SUSESIHUSMOEAC
+XQFTABFD+W+OXQSISMZWTM+BDEXN
TTOWOZC+UTXESULCJG+S+K+.

OJKEPBHVSSYAKGDSW+OESYBNXTTEE
XXOUUXFCATSESULNFUMTCHU+CANNFC
C+EEPVSWLSEV+ETUTMBWCWUN+EDD
CKNQTOURNN+XUNFOU.

On a fait usage d'un *seul* alphabet à *trois* chiffres, mais on a donné *deux* tours de clé.

La traduction de la première phrase est :

« Edgard + Poë + a + dit + que + l + ingéniosité + humaine + ne + peut + rien + cacher + que +

l + ingéniosité + humaine + ne + puisse + découvrir +++ ».

On remarquera que, pour faciliter le travail des déchiffreurs, un groupe de 31 lettres (+ que + l + ingéniosité + humaine + ne + p) a été répété deux fois, ce dont le chiffre n'accuse, du reste, aucune trace.

En terminant, je dédie aux curieux le petit calcul suivant, qui montre bien l'infinie variété des combinaisons dont la cryptographie nouvelle est susceptible.

Si, au lieu d'attribuer les arrangements de chiffres aux lettres, on les attribuait à des groupes de deux lettres, on obtiendrait un nombre considérable de combinaisons et, par suite, de valeurs différentes pour une même lettre.

Nous avons vu, dans le tableau de Vigenère, perfectionné (1re méthode) que le nombre des groupes de deux lettres s'élève à 729, soit 3 à la 6e puissance. Dans la formule $G_n = m^n$, nous pouvons donc faire $m = 3$ et $n = 6$. En d'autres termes, chaque groupe de deux lettres peut être représenté par un arrangement de trois chiffres différents pris 6 à 6.

Mais, d'après le raisonnement que nous avons fait plus haut, il est évident que chacun des chiffres composant un de ces nombres peut être fourni par $243 \times 6 = 1.458$ manières différentes. Chaque groupe de deux lettres possèdera donc

$$1.458^6 = 9.606.056.659.007.943.744,$$

soit plus de $9 \times 10^{18} = 9$ quintillions de valeurs différentes, et chaque lettre, le même nombre

multiplié par 54 ou plus de 518 quintillions de valeurs.

Si ce n'est pas l'indéchiffrabilité absolue, cela en approche, du moins, un peu, et il serait facile d'aller encore beaucoup plus loin, par exemple, en donnant deux tours de clé.

Le système ci-dessus nécessiterait, il est vrai, l'emploi d'un tableau assez long à établir, mais n'offrant cependant aucune difficulté pratique.

---

# APPENDICE

On m'a demandé de démontrer qu'une dépêche cryptographiée selon la méthode exposée ci-dessus ne peut être déchiffrée sans clé.

Bien qu'il soit impossible, en général, de démontrer une négation et qu'on ne puisse même, dans le cas actuel, s'en rapporter à l'expérience, comme le prouvent les déchiffrements merveilleux obtenus notamment par M. le capitaine Bazeries de textes restés indéchiffrables pendant plusieurs siècles, j'ose espérer que les considérations suivantes convaincront les esprits les plus sceptiques qu'employée par des personnes exercées, la *Cryptographie nouvelle* fournit, malgré sa simplicité, des *chiffres absolument incrochetables*.

Remarquons d'abord que, dans les calculs relatifs au nombre des valeurs diverses appartenant à une lettre quelconque, on n'a pas fait intervenir la multiplicité des alphabets dont on dispose.

Il convient de dire que le nombre des alphabets utilisables dans la nouvelle méthode est égal à la somme des permutations formées avec 25 ou 27

lettres, suivant le cas, soit pour l'alphabet *bifide* ou à deux chiffres :

$$1 \times 2 \times 3 \times 4 \times 5 \times 6 \ldots\ldots \times 23 \times 24 \times 25,$$

et pour l'alphabet *trifide* ou à trois chiffres :

$$1 \times 2 \times 3 \times 4 \times 5 \times 6 \ldots \times 24 \times 25 \times 26 \times 27.$$

Avec les alphabets *conjugués*, il faut, pour être exact, élever chacune de ces quantités au carré.

Dans les anciens systèmes, on présente le nombre des permutations possibles comme la *valeur mathématique* de la méthode, bien que, l'alphabet une fois choisi, chaque lettre ne possède qu'une seule et unique valeur et que, pour diversifier, il faille avoir recours à des complications et faire alternativement usage de plusieurs alphabets différents, pour le même cryptogramme.

Dans le nouveau procédé, au contraire, la clé (alphabets et groupements) étant déterminée, la même lettre peut se présenter presque indéfiniment et être, à chaque fois, traduite d'une manière différente, sans qu'il soit nécessaire de modifier le chiffrement en quoi que ce soit.

Le nombre des valeurs que peut, dans chaque cas, prendre un signe quelconque, ayant déjà été calculé, il ne paraît pas utile de le reproduire ici.

Réciproquement, des lettres différentes peuvent fournir le même signe au cryptogramme.

Prenons pour exemple le mot : *Bordeaux*. Chiffrons-le à l'aide de l'alphabet (partiel) suivant, sans nous occuper du groupement, qui se trouvera ainsi égal à *huit :*

A = 321 D = 122 O = 233 U = 112 V = 332

Z = 123  B = 132  E = 223  R = 331  X = 213
Y = 221.

On aura :

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| B | o | r | d | e | a | u | x |
| 1 | 2 | 3. | 1 | 2 | 3. | 1 | 2 |
| 3. | 3 | 3 | 2. | 2 | 2 | 1. | 1 |
| 2 | 3. | 1 | 2 | 3. | 1 | 2 | 3. |
| Z | Z | Z | V | Y | Z | Z | Z |

soit : *Bordeaux* = ZZZVYZZZ.

Maintenant changeons d'alphabet et groupons par 3 et 5, avec les chiffres suivants :

A = 322  D = 132  O = 222  U = 133  Z = 123
B = 111  E = 213  R = 333  X = 211  + = 231.

Il viendra :

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| B | o | r | d | e | a | u | x |
| 1 | 2 | 3. | 1 | 2 | 3. | 1 | 2 |
| 1 | 2 | 3. | 3. | 1 | 2 | 3. | 1 |
| 1 | 2 | 3. | 2 | 3. | 2 | 3 | 1 |
| Z | Z | Z | Z | Z | Z | Z | + |

ou *Bordeaux* = ZZZZZZZ+.

*Bordeaux* ne présente aucune répétition de lettres et son chiffre s'exprime par un signe *sept fois* répété.

Il en serait de même de tout mot ou tout commencement de phrase écrit avec des lettres différentes ; ce n'est qu'une question d'alphabet.

Faisons usage du suivant :

\+ = 112  C = 111  F = 132  N = 333  Q = 131
S = 321  A = 123  E = 122  I = 213  O = 222
R = 113  U = 212.

et cryptographions le mot : *confisquer*, en groupant encore par 3 et 5 :

| | | |
|---|---|---|
| C o n | f i s q u | e r |
| 1 2 3. | 1 2 3. 1 2 | 1 1 |
| 1 2 3. | 3. 1 2 3. 1 | 2. 1 |
| 1 2 3. | 2 3. 1 1 2. | 2 3. |
| A A A | A A A A + | + A |

et nous aurons : *Confisquer* = AAAAAAA++A.

D'autres alphabets auraient pu nous conduire au même résultat. Par exemple, avec celui-ci :

| | | | | |
|---|---|---|---|---|
| + = 232 | C = 222 | F = 231 | N = 333 | Q = 233 |
| S = 312 | A = 213 | E = 221 | I = 123 | O = 111 |
| R = 323 | U = 122, | | | |

on chiffrera encore :

| | | |
|---|---|---|
| C o n | f i s q u | e r |
| 2 1 3. | 2 1 3. 2 1 | 2 3 |
| 2 1 3. | 3. 2 1 3. 2 | 2. 2 |
| 2 1 3. | 1 3. 2 3 2 | 1 3. |
| A A A | A A A A + | + A. |

Remarquons que nous aurions pu prendre, dans le premier cas, Z = 123 et, dans le second, Z = 213 ; nous aurions alors retrouvé le cryptogramme de *Bordeaux* = ZZZZZZZ+ :

*Confisquer* = ZZZZZZZ++Z.

Prenons pour nouvel alphabet :

| | | | | | |
|---|---|---|---|---|---|
| A 111 | I 231 | S 212 | 111 A | 133 N | 231 I |
| C 213 | M 123 | U 222 | 112 D | 211 V | 232 Z |
| D 112 | N 133 | V 211 | 122 O | 212 S | 312 R |
| E 132 | O 122 | X 333 | 123 M | 213 C | 321 H |
| H 321 | R 312 | Z 232 | 132 E | 222 U | 333 X |

et chiffrons, en groupant par 5, 3 et 4 :

| | | | |
|---|---|---|---|
| E c h e c | a u x | m i r m | i d o n s |
| 1 2 3.1 2 | 1 2 3. | 1 2 3.1 | 2 1 1.1 2 |
| 3.1 2 3.1 | 1 2 3. | 2 3.1 2 | 3.1 2 3.1 |
| 2 3.1 2 3 | 1 2 3. | 3.1 2 3. | 1 2.2 3 2 |
| MMMMM | MMM | MMMM | VMMDZ |

La phrase : *Echec aux mirmidons* se traduira donc par *quatorze* M, dont *douze* de suite.

La phrase suivante :

*Oui, être ou n'être pas papa, paraît être la question*, composée de 41 lettres, fournira *trente-un* E, dont *vingt-deux* consécutifs, si on la cryptographie, avec un groupement convenable, à l'aide de l'alphabet :

| | | | | | |
|---|---|---|---|---|---|
| + 121 | I 133 | R 312 | 111 O | 211 B | 311 Q |
| A 213 | J 122 | S 321 | 112 C | 212 D | 312 R |
| B 211 | K 322 | T 231 | 113 L | 213 A | 313 F |
| C 112 | L 113 | U 222 | 121 + | 221 H | 321 S |
| D 212 | M 223 | V 323 | 122 J | 222 U | 322 K |
| E 123 | N 333 | X 131 | 123 E | 223 M | 323 V |
| F 313 | O 111 | Y 331 | 131 X | 231 T | 331 Y |
| G 233 | P 132 | Z 232 | 132 P | 232 Z | 332 W |
| H 221 | Q 311 | W 332 | 133 I | 233 G | 333 N |

On a, en effet :

| | | | | | |
|---|---|---|---|---|---|
| o u i | e t r e | o u n | e t r e | p a s p a | p a |
| 1 2 1. | 1 2 3.1 | 1 2 3. | 1 2 3.1 | 1 2 3.1 2 | 1 2 |
| 1 2 3. | 2 3.1 2 | 1 2 3. | 2 3.1 2 | 3.1 2 3.1 | 3.1 |
| 1 2 3. | 3.1 2 3. | 1 2 3. | 3.1 2 3. | 2 3.1 2 3. | 2 3. |
| +EE | EEEE | EEE | EEEE | EEEEE | EE |

| | | | | | | |
|---|---|---|---|---|---|---|
| pa | ra | it | etre | laque | stio | n |
| 12 | 32 | 12 | 123.1 | 123.21 | 321.1 | 3 |
| 3.1 | 1.1 | 3.3 | 23.12 | 1.112.2 | 23.31 | 3 |
| 23. | 23 | 31. | 3.123. | 33.123. | 1.131. | 3. |
| EE | SE | EY | EEEE | EBCGE | SEQX | N |

Tout autre groupemement fera disparaître les E. Ainsi, en groupant uniformément par 5, il viendra :

++ZRYQTDVEECRYZTBTYZDSQPV+GVX RCKOGRPCGXXN ;

Par 8, on aura :

+EOZRCYTTTJVEERVR+ZFXCVZDEOWR IXGZPOJGXTXN ;

Par 4, 5 et 7, alternativement, on trouvera :

+CSGTE+DRRQZRFRVREXZDSQPV+TITA XGZOMESPYQF ; etc.

Quels indices, quelles chances de déchiffrement, une méthode qui fournit de semblables résultats peut-elle offrir aux Chercheurs ?

Je n'en vois pas et je suis bien persuadé que tous ceux qui prendront la peine de chiffrer une phrase, un simple mot s'ils veulent, avec divers alphabets d'abord, puis avec un seul et des groupements différents, tant simples qu'à double ou triple tour de clé, et enfin en faisant varier tous les éléments, arriveront forcément à la conviction que :

*Par l'emploi d'alphabets et de groupements convenables, il est possible d'assigner à un texte chiffré telle signification que l'on veut.*

Un même cryptogramme peut donc fournir de nombreuses traductions. C'est ce qu'il est facile de constater.

Soit, par exemple à traduire, en groupant par 7 :

DOBCNXK.

A l'aide de l'alphabet *bifide :*

| | | | |
|---|---|---|---|
| A 23 | E 43 | L 24 | T 35 |
| B 41 | H 31 | N 25 | U 13 |
| C 11 | I 51 | O 22 | V 21 |
| D 32 | K 34 | R 14 | X 53 |

| | | | |
|---|---|---|---|
| 11 C | 22 O | 31 H | 41 B |
| 13 U | 23 A | 32 D | 43 E |
| 14 R | 24 L | 34 K | 51 I |
| 21 V | 25 N | 35 T | 53 X |

Nous aurons, en donnant un seul tour de clé :

| | | | | | | |
|---|---|---|---|---|---|---|
| . | . | . | . | . | . | . |
| D | O | B | C | N | X | K |
| 3 | 2 | 2 | 2 | 4 | 1 | 1 |
| 1 | 2 | 5 | 5 | 3 | 3 | 4 |
| H | o | n | n | e | u | r |

Et en donnant deux tours de clé :

| | | | | | | |
|---|---|---|---|---|---|---|
| . | . | . | . | . | . | . |
| D | O | B | C | N | X | K |
| 3 | 2 | 2 | 2 | 4 | 1 | 1 |
| 1 | 2 | 5 | 5 | 3 | 3 | 4 |
| | | | | | | |
| 3 | 1 | 2 | 2 | 2 | 5 | 2 |
| 5 | 4 | 3 | 1 | 3 | 1 | 4 |
| T | r | a | v | a | i | l |

Prenons maintenant l'alphabet *trifide* reproduit ci-après :

| | | | | | | |
|---|---|---|---|---|---|---|
| + 133 | G 111 | O 132 | | 111 G | 133 + | 311 L |
| A 122 | H 323 | R 331 | | 112 B | 211 U | 312 E |
| B 112 | I 212 | U 211 | | 113 N | 212 I | 321 X |
| C 213 | K 123 | V 221 | | 122 A | 213 C | 323 H |
| D 231 | L 311 | X 321 | | 123 K | 221 V | 331 R |
| E 312 | N 113 | | | 132 O | 231 D | |

et recommençons à traduire le même chiffre que précédemment.

Il viendra :

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | · | · | · | · | · | · | · |
| | D | O | B | C | N | X | K |
| | 2 | 3 | 1 | 1 | 3 | 2 | 1 |
| | 1 | 2 | 2 | 1 | 3 | 1 | 1 |
| | 3 | 3 | 2 | 1 | 1 | 2 | 3 |
| au premier tour de clé : | C | h | a | g | r | i | n |
| | 2 | 1 | 3 | 3 | 2 | 3 | 1 |
| | 2 | 2 | 1 | 1 | 1 | 3 | 3 |
| | 1 | 2 | 1 | 2 | 1 | 1 | 3 |
| et au second : | V | a | l | e | u | r | + |

Le nouvel alphabet que voici :

| | | | | | | |
|---|---|---|---|---|---|---|
| + 311 | K 131 | R 333 | | 121 S | 223 A | 322 C |
| A 223 | I 233 | S 121 | | 123 O | 233 I | 323 X |
| B 313 | J 132 | U 221 | | 131 K | 311 + | 331 H |
| C 322 | M 312 | X 323 | | 132 J | 312 M | 333 R |
| D 321 | N 213 | | | 213 N | 313 B | |
| H 331 | O 123 | | | 221 U | 321 D | |

nous donnera :

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | . | . | . | . | . | . | . |
| | D | O | B | C | N | X | K |
| | 3 | 2 | 1 | 1 | 2 | 3 | 3 |
| | 1 | 3 | 3 | 2 | 2 | 2 | 1 |
| | 3 | 3 | 2 | 3 | 1 | 3 | 1 |
| au premier tour : | B | i | j | o | u | x | + |
| | 3 | 1 | 3 | 2 | 3 | 3 | 1 |
| | 3 | 2 | 1 | 2 | 3 | 2 | 2 |
| | 1 | 3 | 2 | 3 | 3 | 1 | 1 |
| et au second : | H | o | m | a | r | d | s |

Avec ce quatrième alphabet :

| | | | | | |
|---|---|---|---|---|---|
| A 232 | I 312 | R 331 | 111 C | 222 B | 322 X |
| B 222 | K 131 | T 122 | 122 T | 223 H | 323 U |
| C 111 | M 313 | U 323 | 131 K | 232 A | 331 R |
| D 132 | N 212 | X 322 | 132 D | 311 Q | 333 O |
| E 211 | O 333 | | 211 E | 312 I | |
| H 223 | Q 311 | | 212 N | 313 M | |

on trouve :

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | . | . | . | . | . | . | . |
| | D | O | B | C | N | X | K |
| | 1 | 3 | 2 | 3 | 3 | 3 | 2 |
| | 2 | 2 | 1 | 1 | 1 | 2 | 1 |
| | 2 | 3 | 2 | 2 | 1 | 3 | 1 |
| au premier tour : | T | u | n | i | q | u | e |
| | 1 | 2 | 2 | 3 | 2 | 3 | 2 |
| | 1 | 2 | 3 | 1 | 2 | 3 | 1 |
| | 1 | 3 | 2 | 3 | 2 | 1 | 1 |
| et au second : | C | h | a | m | b | r | e |

Je m'arrête, de crainte de lasser la patience des lecteurs.

Nous avons trouvé successivement :

DOBCNXK = {
H o n n e u r,
T r a v a i l,
C h a g r i n,
V a l e u r +,
B i j o u x +,
H o m a r d s,
T u n i q u e,
C h a m b r e,

Cela nous fait *huit* traductions différentes du même mot, à l'aide de *quatre* alphabets seulement et *sans modifier le groupement.*

On objectera peut-être que ce qui est possible sur un assemblage de quelques lettres, ne pourrait évidemment pas se produire sur un texte de quelque longueur.

Pour toute réponse, je présenterai un dernier exemple de *dix-sept* lettres, dont aucune n'est répétée.

Soit à traduire en clair :

DGKFAYJHVLXCOZBUN.

En nous servant de l'alphabet qui suit et en groupant par *cinq*,

| | | | |
|---|---|---|---|
| A 41 | H 32 | O 24 | V 54 |
| B 45 | I 52 | P 23 | X 31 |
| C 22 | J 35 | Q 21 | Y 51 |
| D 43 | K 13 | R 44 | Z 53 |
| E 34 | L 33 | S 15 | |
| F 42 | M 55 | T 12 | |
| G 14 | N 25 | U 11 | |

| | | | |
|---|---|---|---|
| 11 U | 23 P | 35 J | 52 I |
| 12 T | 24 O | 41 A | 53 Z |
| 13 K | 25 N | 42 F | 54 V |
| 14 G | 31 X | 43 D | 55 M |
| 15 S | 32 H | 44 R | |
| 21 Q | 33 L | 45 B | |
| 22 C | 34 E | 51 Y | |

il viendra :

| | | | |
|---|---|---|---|
| . . . . . | . . . . . | . . . . . | . . |
| DGKFA | YJHVL | XCOZB | UN |
| 4 3 1 4 1 | 5 1 3 5 3 | 3 1 2 2 2 | 1 1 |
| 3 4 2 4 1 | 2 5 4 3 3 | 4 5 3 4 5 | 2 5 |
| D e t r u | i s e z l | e s p o n | t s |

Tandis qu'en employant sans groupement (Group = 17) cet autre alphabet :

| | | | | | |
|---|---|---|---|---|---|
| + 311 | I 333 | R 213 | 111 V | 211 Q | 311 + |
| A 132 | J 233 | S 223 | 112 C | 212 E | 312 T |
| B 221 | K 232 | T 312 | 113 X | 213 R | 313 W |
| C 112 | L 133 | U 122 | 121 H | 221 B | 321 G |
| D 123 | M 323 | V 111 | 122 U | 222 O | 322 Y |
| E 212 | N 332 | X 113 | 123 D | 223 S | 323 M |
| F 331 | O 222 | Y 322 | 131 P | 231 Z | 331 F |
| G 321 | P 131 | Z 231 | 132 A | 232 K | 332 N |
| H 121 | Q 211 | W 313 | 133 L | 233 J | 333 I |

on obtiendra :

```
. . . . . . . . . . . . . . . . .
D G K F A Y J H V L X C O Z B U N
1 2 3 3 2 1 2 3 2 3 3 1 1 3 2 3 2
2 2 3 3 1 2 1 1 1 1 1 3 3 1 1 3 1
1 2 2 2 2 2 3 1 2 2 1 1 2 2 3 3 2
H o n n e u r + e t + P a t r i e
```

.˙.

Voyons maintenant quelles difficultés rencontrera un déchiffreur essayant de traduire *sans clé* les cryptogrammes de ce système.

D'abord, les anciennes méthodes de déchiffrement sont inapplicables, puisque toute relation est supprimée et tout rapport rompu entre les lettres du *chiffre* et celles du texte *clair*.

Il sera donc indispensable de donner à chaque signe une valeur numérique, ce qui ne peut se faire utilement en l'absence de l'alphabet, dont on ne connaît même pas le type (bifide ou trifide).

Supposons néanmoins ce premier résultat acquis et le *vrai* tableau numérique obtenu. Il faut maintenant grouper, suivant le cas, 2 à 2 ou 3 à 3, les chiffres qui forment ce tableau, chiffres qui se suivent sans ordre connu et semblent jetés au hasard. Leurs répétitions présentant sensiblement la même fréquence, rien ne peut guider le chercheur, rien, exactement rien. Lors même qu'il parviendrait à déterminer les chiffres appartenant à chaque lettre, ces chiffres étant dans un ordre confus, il lui faudrait encore assigner à chacun d'eux sa place respective; or, si deux objets combinés 2 à 2 ne fournissent que deux arrangements, trois objets combinés 3 à 3 en peuvent former six; il resterait donc à choisir, pour chaque lettre, d'une valeur encore inconnue, celui des arrangements qui convient.

Ce travail terminé, par hypothèse, le chercheur n'aura plus à vaincre, pour trouver une traduction, que des difficultés de même nature et de

même ordre que celles résultant de l'emploi des anciennes méthodes.

Admettons donc qu'un déchiffreur émérite parvienne à traduire intégralement un cryptogramme chiffré d'après les nouveaux principes. Alors, il verra se dresser devant lui une difficulté d'un genre tout nouveau et que l'on peut, sans exagération, qualifier d'insurmontable.

Quand, après un labeur plus ou moins long et pénible, on est parvenu à substituer aux signes d'une dépêche chiffrée suivant les anciens systèmes, des lettres offrant un sens clair et précis, on est assuré de posséder la vraie traduction du document.

Tel n'est plus le cas ici. Un même cryptogramme peut admettre un nombre illimité de traductions différentes et, si habile qu'il soit, un déchiffreur ne pourra jamais arriver à la certitude qu'il a découvert le vrai sens de la dépêche interceptée.

Faisons une comparaison pour mieux fixer les idées : un correspondant nous transmet un nombre qu'il tient à laisser inconnu aux intermédiaires. Soit 17 ce nombre, on nous indique 36. Sachant que le nombre qu'on nous envoie est la somme de 19 et du nombre caché, nous n'aurons aucune difficulté à déterminer ce dernier, tandis que ceux qui ne sont pas dans le secret pourront aussi trouver 17, mais rien ne leur fera reconnaître qu'ils sont dans le vrai en le choisissant plutôt qu'en adoptant tout autre.

Nos cryptogrammes sont exactement dans le même cas ; on peut leur attribuer telle signification que l'on veut, dans la limite du nombre des signes employés.

Pour preuve, étudions le dernier exemple.

Il s'agissait de traduire le cryptogramme :

DGKFAYJHVLXCOZBUN

et, à l'aide d'alphabets *simples*, nous avons obtenu :

I. *Détruisez les ponts.*
II. *Honneur + et + Patrie.*

Reprenons la même dépêche et traduisons-la de nouveau.

Pour éviter tant les complications de groupement que les tours de clé multiples, nous ferons usage d'alphabets *conjugués*, et ne grouperons que par 5 ou par 17.

Les alphabets *conjugués* diffèrent des autres seulement en ce que la même lettre peut posséder une valeur numérique différente dans chaque tableau (*chiffrant* et *déchiffrant*).

Que les alphabets soient *bifides* (à deux chiffres) ou *trifides* (à trois chiffres), la manière de procéder reste la même et, en tous points, semblable à celle que nous avons employée jusqu'ici.

Soit les deux alphabets conjugués :

| N° 1 (chiffrant). | | N° 2 (déchiffrant). | | |
|---|---|---|---|---|
| 131 M | 312 E | A 332 | H 113 | U 331 |
| 132 I | 313 + | B 221 | J 121 | V 131 |
| 211 A | 322 R | C 132 | K 133 | X 323 |
| 213 N | | D 122 | L 311 | Y 223 |
| 233 S | | F 111 | N 112 | Z 123 |
| 311 L | | G 233 | O 313 | |

Rappelons d'abord la marche à suivre :

Comme il s'agit d'un *déchiffrement*, nous transformons, à l'aide de l'alphabet n° 2, les lettres de

la dépêche en chiffres que nous écrivons *horizontalement*. Nous les relevons ensuite *verticalement* pour les convertir, de nouveau, en lettres au moyen de l'alphabet n° 1.

Sachant que *cinq* est la base du groupement, nous formons le tableau :

| | | | |
|---|---|---|---|
| . . . . . | . . . . . | . . . . . | . . |
| DGKFA | YJHVL | XCOZB | UN |
| 1 2 2 2 3 | 2 2 3 1 2 | 3 2 3 1 3 | 3 3 |
| 3 1 3 3 1 | 1 1 1 3 1 | 2 3 1 3 1 | 1 1 |
| 1 1 3 3 2 | 3 1 3 1 1 | 2 3 2 2 1 | 1 2 |
| M a s s e | n a+Ma | r s e i l | l e |

et nous trouvons un mot d'ordre :

III. *Masséna + Marseille.*

Avec les alphabets :

N° 1.

| | | |
|---|---|---|
| 13 U | 43 Y | 53 P |
| 21 S | 44 G | 55 O |
| 24 D | 45 T | |
| 32 N | 51 I | |
| 42 A | 52 R | |

N° 2.

| | | | |
|---|---|---|---|
| A 51 | G 41 | N 11 | Y 53 |
| B 23 | H 55 | O 25 | Z 31 |
| C 35 | J 54 | U 22 | |
| D 21 | K 44 | V 24 | |
| F 45 | L 34 | X 32 | |

en groupant par 17, il vient un mot d'ordre différent :

IV. *Duguay-Trouin, Paris.*

En groupant par 5, avec les alphabets :

N° 1.

| | |
|---|---|
| 11 A | 33 T |
| 14 V | 34 E |
| 22 C | 43 D |
| 24 Z | 45 N |
| 32 R | 53 S |

N° 2.

| | | | |
|---|---|---|---|
| A 52 | G 14 | N 23 | Y 32 |
| B 31 | H 44 | O 13 | Z 24 |
| C 33 | J 51 | U 34 | |
| D 11 | K 21 | V 43 | |
| F 41 | L 15 | X 53 | |

il vient :

V. *Avancez sans retard.*

Avec le groupement par 5 et les alphabets :

| N° 1. | | N° 2. | | | |
|---|---|---|---|---|---|
| 12 N | 34 E | A 42 | G 13 | N 41 | Y 33 |
| 15 T | 41 S | B 22 | H 32 | O 51 | Z 52 |
| 22 A | 52 R | C 53 | J 23 | U 34 | |
| 24 Z | 55 O | D 21 | K 12 | V 44 | |
| 32 D | | F 55 | L 24 | X 45 | |

on obtient :

VI. *Attendez des ordres.*

En groupant par 17, les alphabets :

| N° 1. | | N° 2. | | | |
|---|---|---|---|---|---|
| 111 N | 232 Y | A 311 | G 323 | N 222 | Y 232 |
| 113 V | 322 S | B 322 | H 321 | O 332 | Z 312 |
| 122 R | 323 O | C 221 | J 112 | U 333 | |
| 213 D | 333 I | D 211 | K 132 | V 212 | |
| 222 E | | F 231 | L 213 | X 122 | |

nous donnent :

VII. *Envoyons des vivres.*

tandis que, avec le même groupement, ceux-ci :

| N° 1. | | | N° 2. | | | |
|---|---|---|---|---|---|---|
| 12 N | 41 Z | 52 R | A 43 | G 15 | N 52 | Y 55 |
| 13 U | 42 A | 55 O | B 11 | H 25 | O 32 | Z 35 |
| 21 I | 43 T | | C 41 | J 24 | U 31 | |
| 23 L | 44 E | | D 45 | K 14 | V 13 | |
| 33 P | 51 S | | F 42 | L 53 | X 22 | |

fournissent :

VIII. *Tournez la position.*

Il serait fastidieux de continuer plus longuement, mais n'ayant pas craint d'ajouter aux qualités que, selon les spécialistes les plus autorisés, doit réunir tout système de cryptographie pour être réellement utile dans les opérations militaires, la condition que ce système puisse fournir des dépêches qui, *même en partie traduites*, restent inviolables, il est intéressant de s'assurer si cette condition peut être remplie avec les moyens dont nous disposons.

D'un autre côté, les maîtres en l'art cryptographique, MM. Kerckhoffs, Josse, Mamy, de Viaris, etc., recommandent formellement aux déchiffreurs de s'entourer de tous les renseignements qu'ils pourront se procurer au sujet des cryptogrammes qu'ils sont chargés de déchiffrer. En cas de guerre, l'ennemi s'efforcerait certainement, par tous les moyens possibles, de se procurer la clé de nos *chiffres* militaires.

Voyons donc quel est, à cet important point de vue, la valeur de la *Cryptographie nouvelle.*

Supposons que l'ennemi, après avoir intercepté notre dépêche, ait aussi réussi à s'emparer d'une partie des alphabets ayant servi à la cryptographier et qu'il sache d'ailleurs que la base du groupement est *dix-sept.*

Avec les alphabets suivants, dont il connaît l'emploi :

| N° 1. | | N° 2. | | | |
|---|---|---|---|---|---|
| 112 V | 311 Z | A 222 | G 112 | N 121 | Y 221 |
| 211 + | 323 A | B 131 | H 311 | O 323 | Z 211 |
| 212 E | | C 1.. | J 1.3 | U 231 | |
| 213 I | | D ..3 | K 322 | V 132 | |
| 231 L | | F 321 | L 111 | X 331 | |

il n'aura pas de peine à établir le diagramme :

```
. . . . . . . . . . . . . . . . .
D G K F A Y J H V L X C O Z B U N
. . 3 1 1 2 3 2 2 3 2 1 2 2 2 2 2
1 1 . 3 3 1 1 1 3 2 1 1 1 3 3 1 1
. . 3 2 3 2 1 1 1 3 1 2 3 1 1 2 1
. . . . . e z + l a + v i l l e +
```

Il ne manque que 5 chiffres (*cinq tiers de lettres*) sur 51 et la dépêche reste *impénétrable*.

En effet, en admettant, pour l'alphabet n° 1 :

132 = U, 133 = P, 312 = O et 313 = C,

et pour le n° 2 :

C = 123, D = 333 et J = 113,

on traduira :

IX. *Occupez + la + ville +.*

Mais, en supposant, pour le n° 1 :

132 = C et 133 = U,

et, pour le n° 2 :

C = 122, D = 213 et J = 123,

il viendra :

X. *Evacuez + la + ville +*,

ce qui ne présente pas précisément le même sens.

Il n'est peut-être pas sans intérêt de constater que l'ignorance d'*un seul* chiffre de l'alphabet n° 2 peut parfois rendre impossible la lecture d'une dépêche, lorsque l'alphabet n° 1 est incomplètement connu.

Ainsi, prenons pour le n° 2 :

C = 123, D = 3.3 et J = 113,

nous obtiendrons le diagramme :

```
. . . . . . . . . . . . . . . . .
D G K F A Y J H V L X C O Z B U N
3 . 3 1 1 2 3 2 2 3 2 1 2 2 2 2 2
1 1 1 3 3 1 1 1 3 2 1 1 1 3 3 1 1
2 3 3 2 3 2 1 1 1 3 1 2 3 1 1 2 1
. . . . . e z + l a + v i l l e +.
```

La combinaison 323 représentant O, D ne peut avoir pour valeur que 313 ou 333.

En faisant D = 333, on trouve, comme nous l'avons vu :

*Occupez + la + ville +.*

Tandis qu'en posant D = 313 et en complétant l'alphabet n° 1 par :

113 = O, 132 = R, 133 = N, 312 = T et 313 = U,

on lira :

XI. *Tournez + la + ville +.*

Un chiffre manquant sur 51 a donc suffi pour rendre la dépêche inintelligible.

Cette traduction multiple peut sembler un cas exceptionnel ; pour prouver par expérience qu'il n'en est rien, appliquons, toujours à la même dépêche, les nouveaux alphabets :

N° 1.

| | | |
|---|---|---|
| 11 A | 25 V | 45 R |
| 13 O | 34 N | 55 M |
| 15 E | 41 U | |
| 22 I | 42 P | |
| 23 S | 44 T | |

N° 2.

| | | | |
|---|---|---|---|
| A 21 | G 32 | N 53 | Y 44 |
| B .2 | H 11 | O 43 | Z .. |
| C 23 | J 22 | U .5 | |
| D 54 | K 42 | V 25 | |
| F 13 | L 14 | X 24 | |

En groupant par 17, nous aurons :

. . . . . . . . . . . . . . . . . . . .
DGKFAYJHVLXCOZBUN
5 4 3 2 4 2 1 3 2 1 4 4 2 2 1 1 2
5 1 4 2 4 2 3 4 3 . . . 2 . 5 5 3
M u n i t i o n s . . . i . é e s

Il ne nous manque que *trois* lettres, ou plus exactement *quatre* chiffres (sur 34) de l'alphabet n° 2 et la dépêche est encore *indéchiffrable*, bien qu'on en devine à peu près le sens et que l'alphabet n° 1 soit complètement connu.

En faisant :

B = 12, U = 35 et Z = 52,

on lit :

XII. *Munitions épuisées.*

Mais, avec

B = 52, U = 55 et Z = 15,

on trouve l'inverse :

XIII. *Munitions arrivées.*

En modifiant seulement quelques chiffres dans les derniers alphabets, on trouverait, au lieu de

*Munitions arrivées,*
ou *épuisées,*
*Munitions avariées,*
*enlevées,*
*envoyées*, etc., etc.

Remarquons, en outre, qu'il est plus facile à

notre adversaire de connaître la traduction d'une dépêche que de se procurer les alphabets qui ont servi à la cryptographier. Dans ce cas, les difficultés qu'il rencontre sont d'un ordre tout différent.

D'abord, il n'est jamais certain d'avoir la traduction même du chiffre intercepté, des lettres *nulles* pouvant avoir été introduites pour dissimuler le nombre exact des signes de la dépêche ; ces derniers peuvent aussi avoir été transposés, etc.

Admettons cependant qu'il n'existe aucune complication, que l'ennemi a pu s'emparer de notre cryptogramme portant une partie de la traduction et qu'il essaie d'en découvrir la clé.

Soit

DGKFAYJHVLXCOZBUN
Munitions . . . . . ent,

le document détourné.

Un déchiffreur supposant qu'on a employé des alphabets *bifides conjugués* et groupé par 17, arrive à déterminer les alphabets :

| N° 1. | | N° 2. | | | |
|---|---|---|---|---|---|
| 11 T | 34 N | A 51 | G 35 | N 41 | Y 43 |
| 14 A | 42 B | B 24 | H 23 | O 44 | Z 42 |
| 21 M | 45 D | C 32 | J 34 | U 55 | |
| 25 E | 53 I | D 25 | K 15 | V 11 | |
| 32 O | 54 U | F 33 | L 54 | X 31 | |

et à traduire :

XIV. *Munitions abondent.*

Un second déchiffreur, revisant le travail du

premier et faisant les mêmes suppositions, parvient aux alphabets :

| N° 1. | | N° 2. | | | |
|---|---|---|---|---|---|
| 11 T | 34 N | A 42 | G 32 | N 41 | Y 13 |
| 14 A | 35 O | B 43 | H 23 | O 44 | Z 14 |
| 21 M | 43 Q | C 35 | J 45 | U 55 | |
| 23 I | 44 S | D 25 | K 12 | V 11 | |
| 25 E | 55 U | F 33 | L 54 | X 31 | |

et traduit :

XV. *Munitions manquent.*

Quel résultat pourra donner l'application de ces alphabets à une autre dépêche, quand ils sont inaptes à préciser le vrai sens du cryptogramme dont ils sont déduits ?

Comment, si habile qu'il soit, un déchiffreur pourra-t-il se reconnaître au milieu de tant de solutions différentes et même contradictoires ?

Comment pourra-t-il se flatter d'avoir saisi le vrai sens de la dépêche soustraite ?

Et n'est-il pas bien de circonstance cet ironique défi que produit la réunion des deux traductions suivantes :

XVI. + *Devine si tu peux et*

XVII. *choisis si tu l'oses* + ?

Le groupement étant de *cinq* dans les deux cas, le n° XVI est donné par les alphabets :

| N° 1. | | | N° 2. | | | |
|---|---|---|---|---|---|---|
| 111 N | 212 E | 331 X | A 233 | G 132 | N 322 | Y 123 |
| 113 V | 223 D | | B 231 | H 121 | O 313 | Z 332 |
| 121 + | 232 T | | C 133 | J 321 | U 221 | |
| 132 P | 313 I | | D 122 | K 211 | V 312 | |
| 133 U | 322 S | | F 113 | L 232 | X 112 | |

et le n° XVII par ceux-ci :

| N° 1 | | N° 2 | | | |
|---|---|---|---|---|---|
| 112 C | 231 L | A 132 | G 331 | N 223 | Y 333 |
| 123 + | 313 I | B 122 | H 221 | O 322 | Z 131 |
| 132 T | 321 O | C 323 | J 311 | U 312 | |
| 133 U | 322 S | D 133 | K 321 | V 332 | |
| 212 E | 332 H | F 222 | L 232 | X 123 | |

Pour terminer, groupons une dernière fois par *cinq* et les alphabets :

| N° 1 | | | N° 2 | | | |
|---|---|---|---|---|---|---|
| 112 R | 212 E | 323 S | A 222 | G 223 | N 122 | Y 113 |
| 122 C | 231 L | | B 213 | H 121 | O 323 | Z 331 |
| 123 O | 232 T | | C 212 | J 313 | U 231 | |
| 131 N | 311 + | | D 221 | K 123 | V 232 | |
| 133 U | 312 Z | | F 112 | L 312 | X 111 | |

feront apparaître l'invitation :

XVIII. *Lecteurs + concluez.*



1234. — PARIS. — IMP. P. DUBREUIL, 18 A 18 BIS, RUE DES MARTYRS